Summary Report on AICTE Sponsored ATAL FDP on "Cybersecurity Vulnerabilities & Safeguards"

Duration: **1 Week – 14.05.2020 to 18.05.2020**

Conducted by: **National Institute of Technical Teachers Training and Research**

Attendees: **Dr. Vigilson Prem M and Ms. Indra Priyadharshini S**

What is Cyber Security?

Cybersecurity is the practice of protecting networks, systems, hardware and data from digital attacks. Our guide will bring you up-to-speed on the field of cybersecurity, including types of cyber attacks and it's growing global importance in a digital world.

Why Cyber Security is important?

Cybersecurity's importance is on the rise. Fundamentally, our society is more technologically reliant than ever before and there is no sign that this trend will slow. Personal data that could result in identity theft is now posted to the public on our social media accounts. Sensitive information like social security numbers, credit card information and bank account details are now stored in cloud storage services like Dropbox or Google Drive.

The fact of the matter is whether you are an individual, small business or large multinational, you rely on computer systems every day. Pair this with the rise in cloud services, poor cloud service security, smartphones and the Internet of Things (IoT) and we have a myriad of cybersecurity threats that didn't exist a few decades ago. We need to understand the difference between cybersecurity and information security, even though the skillsets are becoming more similar.

How it is going to benefit our students?

As every corporate company is planning to setup security operation system or already having one, there is a huge demand for the job opportunities in security domain. Also we have a centre of excellence in cybersecurity, this FDP would be helpful for training them. And also it would be helpful for our research work.

Day 1 – FN Session

Speaker: **Mr. Ch. A.S. Murthy, CDAC, Hydreabad**

Topic: **Cyber Crime Scenario: Global & India Perspective**

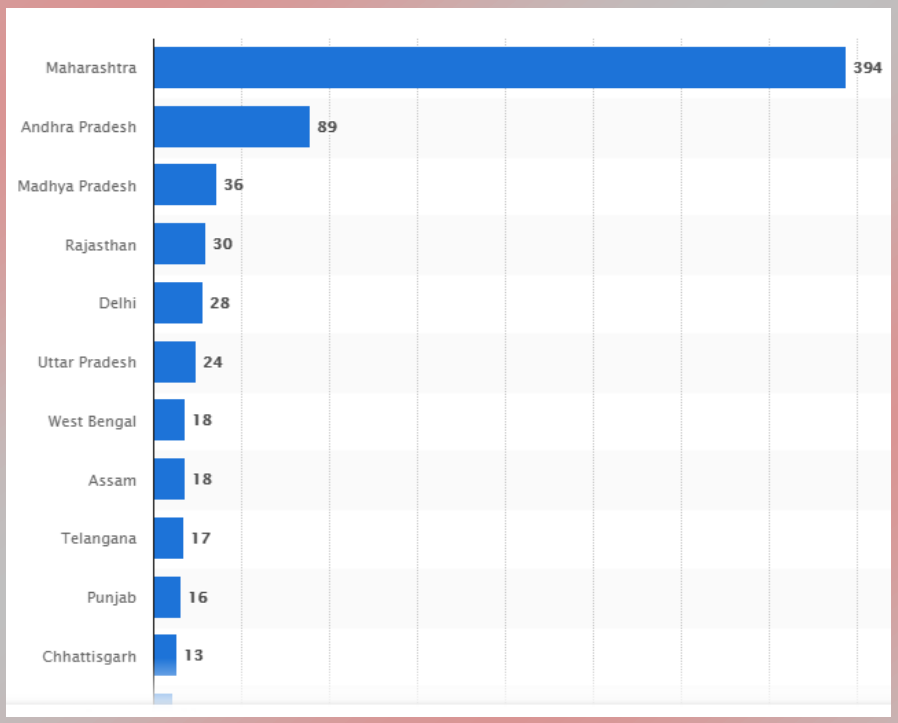
These days' computer and internet become very Necessary and useful for our daily life. Today the internet is the great mediator of our lives. In present days people can get information, store information and share information through the internet. Back 20's years later there was approx.100000 people uses internet but now around 3,405,518,376 people are surf the net around the globe. The growing fastest world of internet is known as cyber world. Today cyber world are fastest moving and high technology world. Asian countries are most uses of internet in the world.

What is Cyber Crime?

As per the Information Technology (amendment) Act 2008, the Indian Cyber law. "Cyber terrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against property, government and people at large." OR "Acts those are punishable by the Information Technology Act"

- ***No. of Cyber Crimes against Women and Children across India in 2018:***

Source: https://www.statista.com/statistics/1097724/india-cyber-stalking-bullying-cases-against-women-children-by-leading-state/



- ***India stands third among top 20 cyber crime victims, says FBI report***

Current Protection provided under Indian Legal Framework against cybercrime
The protection to combat cybercrime is twofold:

- The Information Technology Act, 2000
- Indian Penal Code of 1860.

For crimes like email account hacking, credit card fraud, web defacement, introduction of virus, phishing and email scams, source code theft and theft of confidential information, the protection is available under the IT Act, 2000. Though IT Act does not expressly define cyber-crime but include both cyber-crimes and cyber contraventions. The important provision related to cybercrime and their punishments are as following:

Sections	**Particulars**	**Punishment for the offence**
Section 43	Damage to Computer system etc.	Compensation to the person affected.
Section 66	Computer related offence	Imprisonment for term of 3 years or fine for 5 lakh rupees or both.
Section 67	Publication or transmission of obscene material in e-form	Fine of 5 lakh rupees, and imprisonment of 3 years and double conviction on second offence
Section 68	Not complying with directions of controller	Fine up to 1 lakh or imprisonment of 2 years or both.
Section 70	Protected System	Imprisonment up to 10 years and shall also be liable for a fine.
Section 72	Breaking confidentiality of the information of computer	Imprisonment for term of 2 years or fine of 1 lakh rupees or both.
Section 73	Publishing of false digital signatures	Imprisonment for term of 2 years or fine for 1 lakh rupees or both
Section 74	Publication of digital signature for fraudulent purpose	Imprisonment for term of 2 years or fine for 1 lakh rupees or both.

Day 1 – AN Session:

Speaker: **Mr. Amrendra Sharan, NITTTR, Chandigarh**

Topic: **OWASP Top 10 Security Risks, Vulnerability Assessment and Penetration Testing, IT Security Audit**

Need of Website

(Image source : https://www.carpet-cleaning-equipment.net/images/websites/website.png)

Need of Website Security

HOME | MARKETS | COMPANIES | OPINION | TECH | SPECIALS | PF | PORTFOLIO | MULTIMEDIA | BUDGET 2020 | SPORTS | COVID-19

Business Standard

Beyond Business GO

21,467 Indian websites were hacked in Jan-Oct period, show CERT-In data

Minister of State of Electronics and IT, there have been attempts from time to time to launch cyber attacks on Indian cyber space

Press Trust of India | New Delhi
Last Updated at December 11, 2019 19:46 IST

Representative image of hackers

Over 21,400 Indian websites were hacked this year up to October, Parliament was informed on Wednesday.

"As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In), a total number of 33,147, 30,067, 17,560 and 21,467 Indian websites were hacked during the year 2016, 2017, 2018 and 2019 (till October), respectively," Minister of State for Electronics and IT Sanjay Dhotre said in a written reply

LATEST NEWS

IN THIS SECTION | ALL

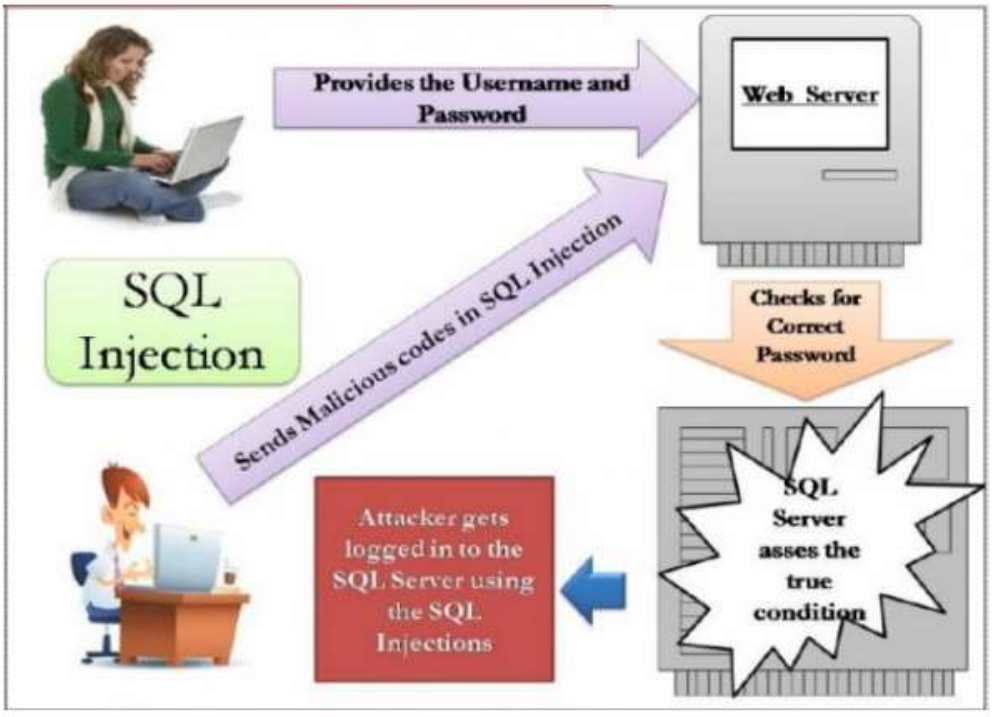
Sell unsold units at 'no-profit-no-loss' to boost liquidity: Nitin Gadkari

Types of Security attacks

High Risk Web application vulnerabilities:

- SQL Injection
- XSS (Cross Site Scripting)
- Sensitive data exposure
- Malicious file upload
- Security misconfigurations (Directory listing)

SQL Injection



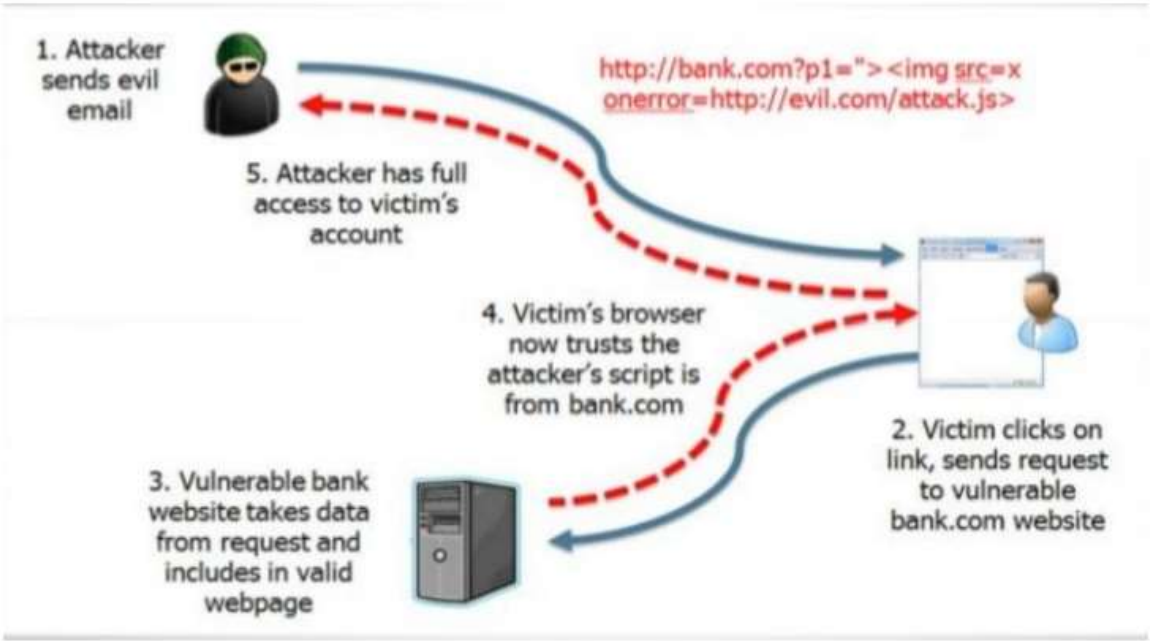
(Image source https://www.slideshare.net/anurag424242/introduction-to-web-application-penetration-testing)

Cross site scripting (XSS)

- Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to upload, post, or send malicious content such as comments, images, or messages (usually in the form of Javascript).

- Because a browser cannot know if the script should be trusted or not, it will execute the script in the user context allowing the attacker to perform unusual action (e.g. phishing page, running a set of commands, or even stealing login session cookie)

Traditional XSS/ Reflected



(Image source https://www.slideshare.net/anurag424242/introduction-to-web-application-penetration-testing)

Day 2 – FN Session

Speaker: **Sh. Gurucharan Singh, CDTI, Ministry of Home Affairs, India**

Topic: **Forensic Tools for Investigation – Case Study Approach**.

I personally found this session very interesting. The speaker explained about cyber crime investigation with live examples and realtime case studies. We came to know about various forensic tools used by the Cyber Crime Police and the method of investigation. He also gave many insights about individuals personal security measures and tools for being safe in the internet.

OPEN SOURCE TOOLS FOR THE DIGITAL FORENSICS

THE FAMOUS PAID TOOLS USED BY FORENSIC SCIENTISTS

- **Encase – For extraction and analysis of Storage Devices**
- **UFED – For extraction and analysis of Cellphone**
- **XRY – for extraction and analysis of cellphone**

FREE OPEN SOURCE TOOLS

Domains lookup

- **Website.informer.com**
- **www.who.is**
- **www.domaintools.com**
- **www.dnsstuff.com**
- **www.cqcounter.com/whois**
- **In.godaddy.com/whois**

Tinyurl/bit.ly link expander http://checkshorturl.com/

EXIF FILE/METADATA VIEWER - http://exif.regex.info/exif.cgi

CHECK YOUR EMAIL WHETHER COMPROMISED

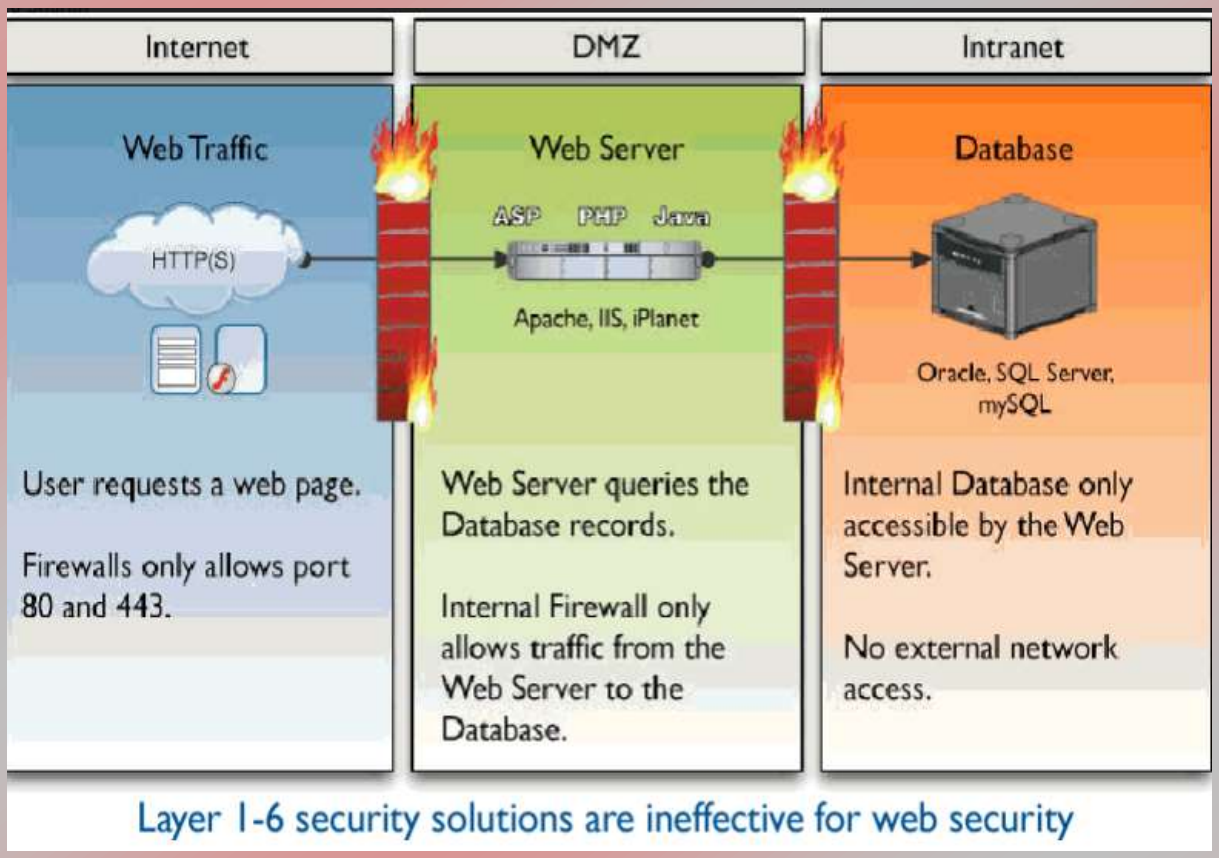
https://haveibeenpwned.com/.

Email header analysis http://ip2location.com/free/email-tracer

Day 2 – AN Session

Speaker: **Mr. Amrendra Sharan, NITTTR, Chandigarh**

Topic: **Hands on VAPT, Setting up DUVWA, OS Fingerprinting, Banner Grabbing, Brute Force Attack, OS Command Injection**



Layer 1-6 security solutions are ineffective for web security

Website Security Audit process

Patching Vulnerabilities & Certification

- Based on the audit report developer team will patch all the vulnerabilities and submit the web application for re-assessment.
- If all findings are patched auditor will issue a certificate or Web Site Security Seal.
- This seal Improves the website visitor's confidence and credibility.

Certification or Seal

Day 3 – FN Session

Speaker: **Dr. Mala Kalra, NITTTR, Chandigarh**

Topic**: Symmetric Key Cryptography – DES**

Speaker explained in detail about Symmetric Key Crypto System, CryptAnalysis & Data Encryption Standard Algorithm.

Text Book Author for Reference: William Stallings

Day 3 – AN Session

Speaker: **Mr. Amrendra Sharan, NITTTR, Chandigarh**

Topic: **Hands on VAPT- SQL Injection and XSS attacks**

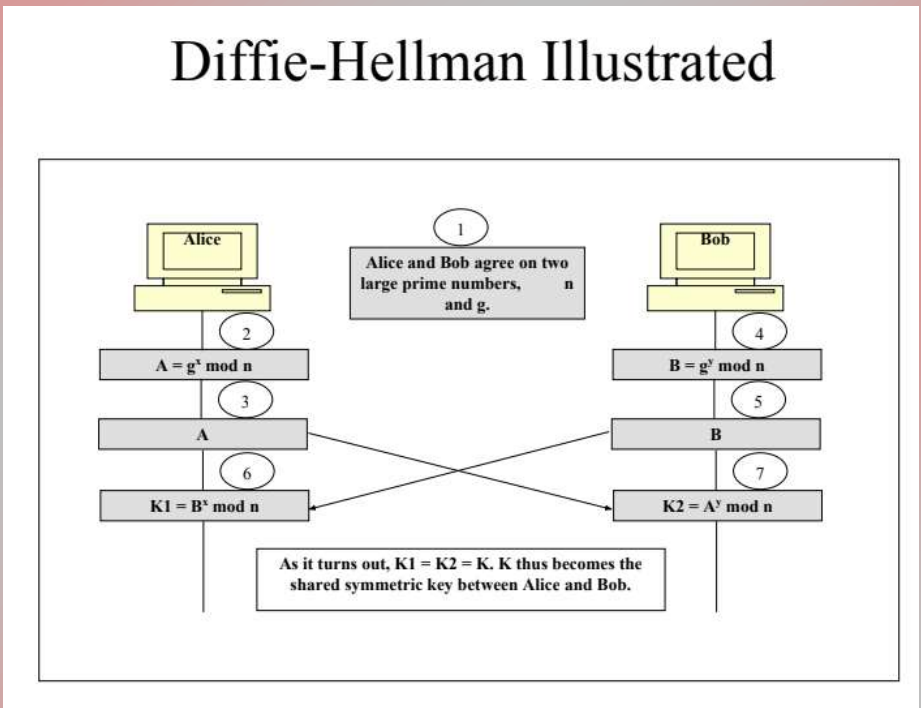
Speaker explained about various reflected XSS payloads, SQL/Bind SQL Injection Payloads and demonstrated various attacks in DUWA network.

Day 4 – FN Session

Speaker: **Dr. C. Ramakrishna, NITTTR, Chandigarh**

Topic: **Challenges in Symmetric Key Cryptography & Solutions**

Speaker explained about the practical difficulties and challenges in the symmetric key cryptography. He explained Diffie Hellman Cryptography as the solution for Key Determination. He also explained RSA Algorithm – public key cryptography. We solved several problems on these topics.



RSA Algorithm
(thanks to Rivest, Shamir,Adleman)

1. Choose two large prime numbers P and Q $(P \neq Q)$
2. Calculate N = P x Q
3. Select the public key (i.e. the encryption key) E such that it is not a factor of
   $(P - 1) \times (Q - 1)$; $1 < E < (P-1)(Q-1)$; $\gcd(E, (P-1)(Q-1)) = 1$
4. Select the private key (i.e. the decryption key) D such that the following equation is true:
   $ED = 1 \pmod{(P - 1) \times (Q - 1)}$
   Therefore, Public key = {E,N} and Private key = {D,N}
5. For encryption, calculate the cipher text CT from the plain text PT as follows:
   $CT = PT^E \bmod N$
6. Send CT as the cipher text to the receiver
7. For decryption, calculate the plain text PT from the cipher text CT as follows:
   $PT = CT^D \bmod N$

Extended Euclid's Algorithm (Ø(N),E)

1. (A1, A2, A3) ←(1, 0, Ø(N)); (B1, B2, B3)←(0,1,E)
2. if B3 = 0 return A3 = gcd(Ø(N), E); no inverse
3. if B3 = 1 return B3 = gcd(Ø(N), E); B2 = E^{-1} mod Ø(N)
4. Q = $\left\lfloor \frac{A3}{B3} \right\rfloor$ ---- Quotient
5. (T1, T2, T3) ← (A1 – QB1, A2 – QB2, A3 – QB3)
6. (A1, A2, A3) ← (B1, B2, B3)
7. (B1, B2, B3) ← (T1, T2, T3)
8. goto 2

Day 4 – AN Session

Speaker: **Mr. Amrendra Sharan, NITTTR, Chandigarh**

Topic: **Hands on VAPT- CSRF Attack and XXE Attack**

Speaker practically demonstrated the CSRF attack and XXE attak using DUVWA framework.

Day 5 – FN Session

Speaker: **Dr. Ashu Sharma, MindTree, Hyderabad**

Topic: **Introduction to First Generation Malware , Malware Analysis, Tools for Malware Detection, Mitigation and Analysis**

Speaker explained about First Generation Malwares, how malwares can be detected, how files are analysed for malware infection, how it can be mitigated. Practical demonstrations were shown.

Day 5 – AN Session

Speaker: Mr**. Vipin Gupta, U-Net Solution**

Topic: **Implementation & Setting up of Firewalls in an Organization**

Available Firewalls

* Cisco ASA (adaptive security appliance)

* Checkpoint Firewall

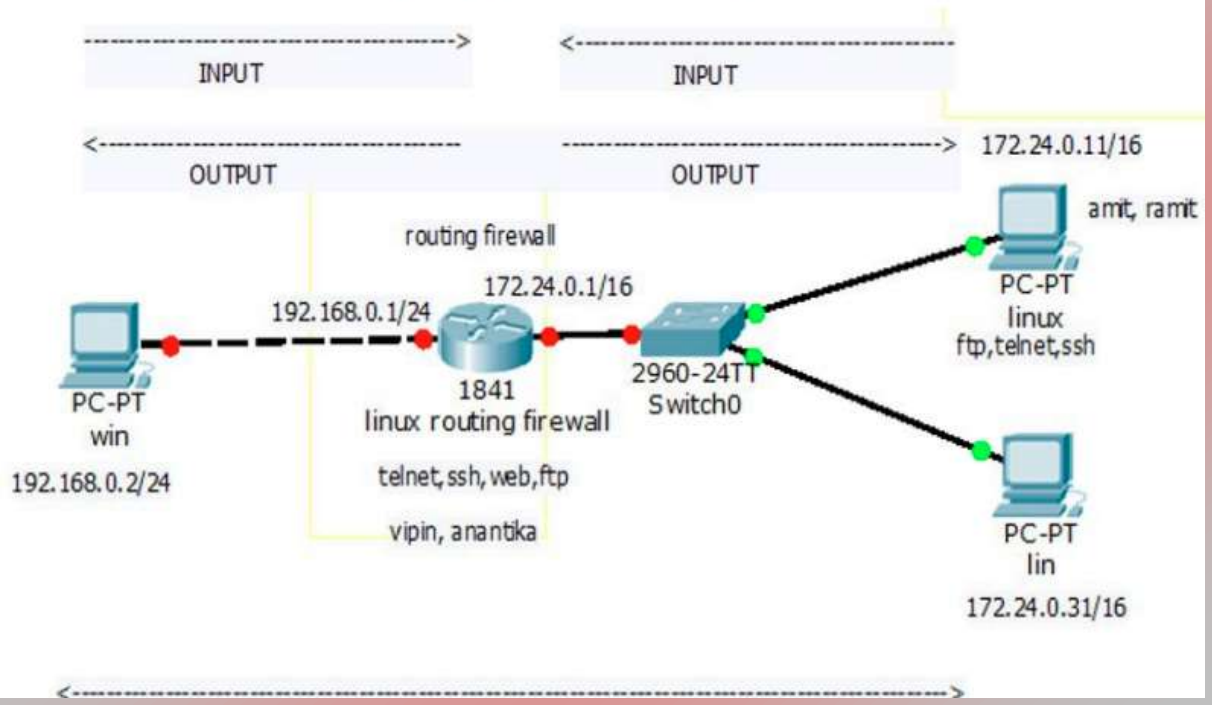
* Microsoft ISA

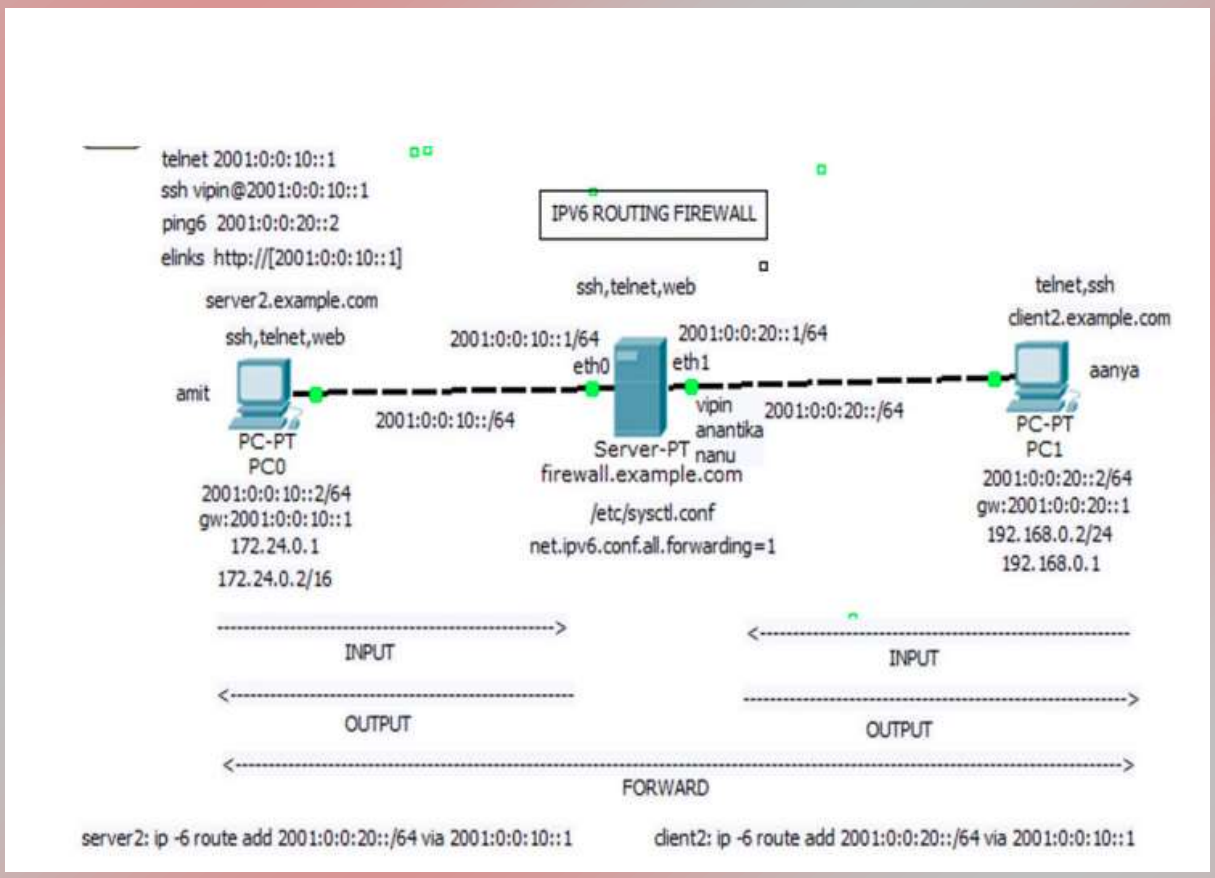
Microsoft Internet Security & Acceleration Server

* Linux based Netfilter iptables Firewall

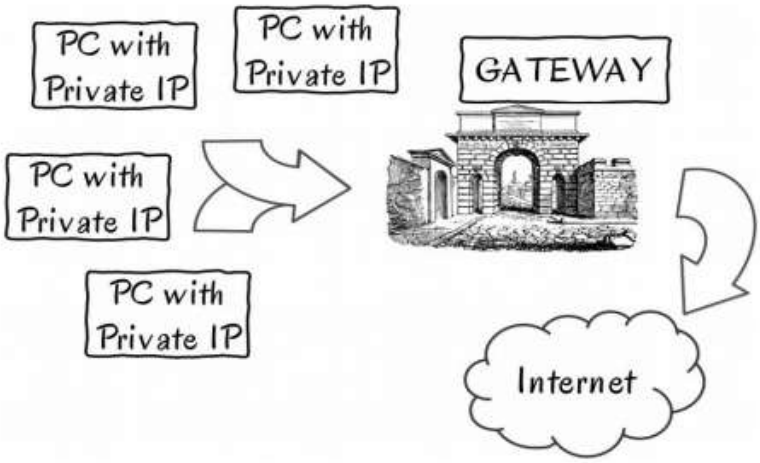
Iptables

Direction of Firewall




telnet 2001:0:0:10::1
ssh vipin@2001:0:0:10::1
ping6 2001:0:0:20::2
elinks http://[2001:0:0:10::1]
IPV6 ROUTING FIREWALL
server2.example.com
ssh,telnet,web
ssh,telnet,web
2001:0:0:10::1/64
eth0
2001:0:0:20::1/64
eth1
telnet,ssh
client2.example.com
aanya
amit
2001:0:0:10::/64
vipin
anantika
nanu
2001:0:0:20::/64
PC-PT
PC0
2001:0:0:10::2/64
gw:2001:0:0:10::1
172.24.0.1
172.24.0.2/16
Server-PT
firewall.example.com
/etc/sysctl.conf
net.ipv6.conf.all.forwarding=1
PC-PT
PC1
2001:0:0:20::2/64
gw:2001:0:0:20::1
192.168.0.2/24
192.168.0.1
INPUT
INPUT
OUTPUT
OUTPUT
FORWARD
server2: ip -6 route add 2001:0:0:20::/64 via 2001:0:0:10::1
client2: ip -6 route add 2001:0:0:20::/64 via 2001:0:0:10::1

SNAT/DNAT


PC with Private IP
PC with Private IP
GATEWAY
PC with Private IP
PC with Private IP
Internet


10.1.10.5
Private
10.1.10.1
Public
1.1.70.5
Internet
Destination NAT

Day 6 – FN Session

Speaker: Ms**. Sumedha Talwar, Art of Living**

Topic: **Stress Management, Meditation, Health and Happiness**

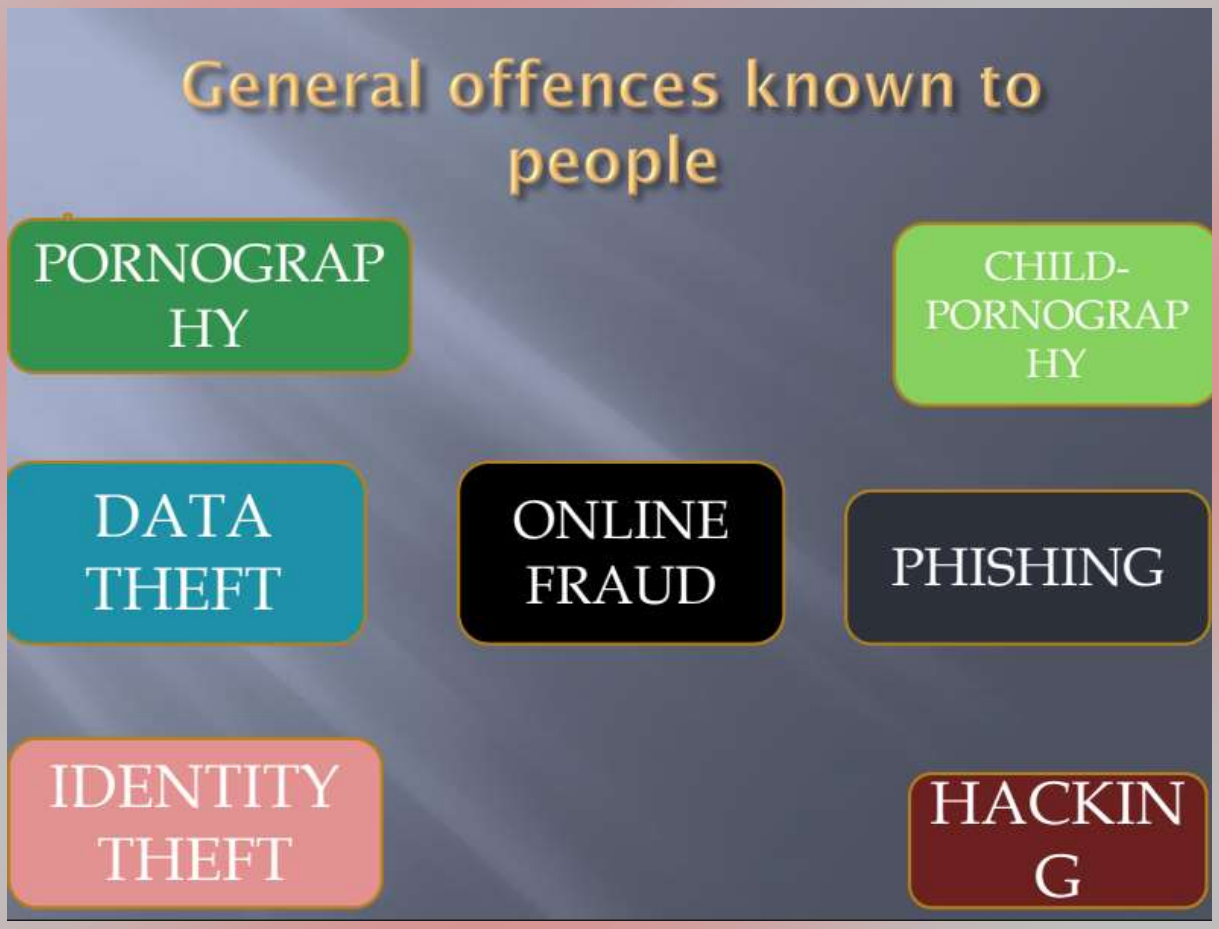
Speaker taught Meditation and importance of breathing, yoga to lead a no-stress, peaceful life.

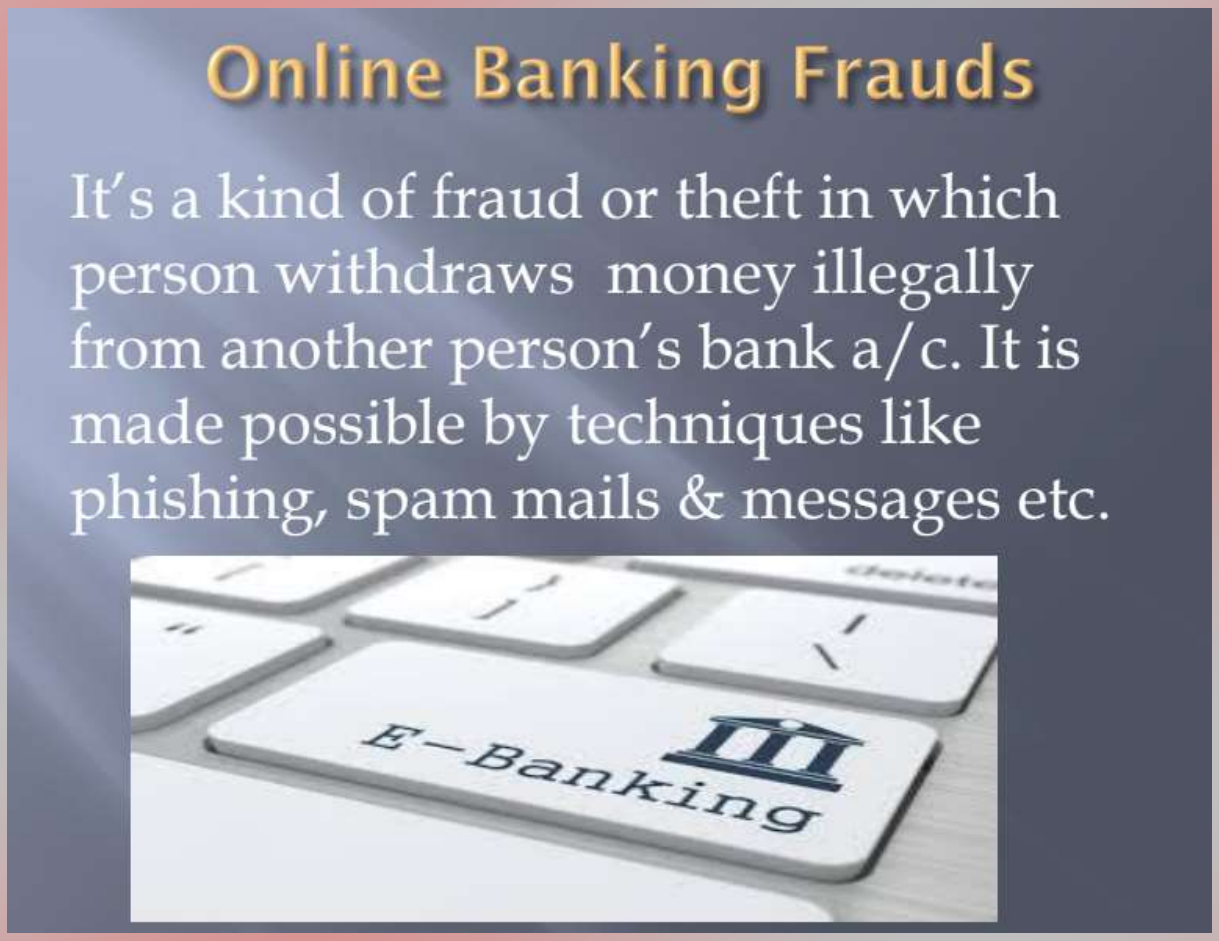
Day 6 – AN Session

Speaker: **Advocate Sh. Akhilesh Vyas, High Court Punjab & Haryana**

Topic: **IT Act 2000 : Case Study Approach**


netmeds
India Ki Pharmacy
zomato
paytm
bigbasket
amazon
Uber
bookmyshow


General offences known to people
PORNOGRAPHY
CHILD-PORNOGRAPHY
DATA THEFT
ONLINE FRAUD
PHISHING
IDENTITY THEFT
HACKING



The FDP was concluded with an assessment, feedback session and valedictory function.

Thanks!