

**Title: SESSION ON NETWORK SECURITY APPLICATIONS**

**Date: 22<sup>nd</sup> February, 2019**

**Time: 11.15 to 1.15pm**

**Class: T.E. Computer Engg. Students**

**Venue: IBM Lab, A-Wing 2nd Floor, Department of Computer Engg., DBIT**

**Faculty In-charge: Shafaque Fatma Syed**

The Cyber Security Session organized by Department of Computer was held on 22nd February 2019. It started at 11:15am by an introductory speech by Prof. Shafaque Syed. The session was further led by the speaker Mr. Pratik Chotaliya (Certified ethical hacker, Security Expert) on an interactive session focusing on topics like:

- Network Security
- Denial of Service(DOS)
- Internet Security Protocol

The session started by introduction to the various internal and external security threats on a system. Emphasizing the importance of Confidentiality, Integrity and Availability in area of Security and also how Vulnerability is weakness of a Secured System was explained. Concepts involving the following was illustrated:

- ARP Poisoning (ARP Spoofing) – A technique by which an attacker sends (spoofed) Address Resolution Protocol (ARP) messages onto a local area network. Generally, the aim is to associate the attacker's MAC address with the IP address of another host, such as the default gateway, causing any traffic meant for that IP address to be sent to the attacker instead.
- Packet Sniffing/Spoofing – The act of capturing packets of data flowing across a computer network. Packet sniffing is widely used by hackers and crackers to gather information illegally about networks they intend to break into.
- Port Scanning – To check server side ports and services by NMap and TCP 3 way handshake. A process that sends client requests to a range of server port addresses on a host, with the goal of finding an active port. The majority of uses of a port scan are not attacks, but rather simple probes to determine services available on a remote machine.

- UDP Scan - A UDP packet is sent to a port that is not open, the system will respond with an ICMP port unreachable message. Most UDP port scanners use this scanning method, and use the absence of a response to infer that a port is open. However, if a port is blocked by a firewall, this method will falsely report that the port is open. If the port unreachable message is blocked, all ports will appear open.
- TCP Syn Flood – A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic. The basis of the SYN flooding attack lies in the design of the 3-way handshake that begins a TCP connection. In this handshake, the third packet verifies the initiator's ability to receive packets at the IP address it used as the source in its initial request, or its return reachability.
- Hacking Android Application by use of Oracle VM VirtualBox, Windows VM Virtual Box where Android emulator would run, Kali Linux – VM image, Android SDK, Metasploit Framework
- ICMP flooding – Ping flood, also known as ICMP flood, a common Denial of Service (DoS) attack in which an attacker takes down a victim's computer by overwhelming it with ICMP echo requests, also known as pings. The attack involves flooding the victim's network with request packets, knowing that the network will respond with an equal number of reply packets.

The various kinds of DOS attacks like ICMP, SYN, UDP, DDOS was explained and how to differentiate between the operating system used by the target server, by the value of time to live (ttl) was demonstrated.

This session ended at 1pm and aimed to provide an opportunity to students to connect the **theoretical knowledge of CSS** with a **practical application of how it's actually works** for better understanding of Security within System.

Report prepared by-

Atharva Deshmukh



**DON BOSCO INSTITUTE OF TECHNOLOGY**  
DEPARTMENT OF COMPUTER ENGINEERING

**WORKSHOP ON NETWORK SECURITY APPLICATIONS**  
ATTENDANCE SHEET

**CLASS: T.E.      DATE: 22/02/2019**  
**SUBJECT: CRYPTOGRAPHY AND SYSTEM SECURITY**

**TIME: 11AM TO 1PM**  
**VENUE: COMP LAB - 4**

ROLL NO	NAME OF STUDENT	SIGNATURE
40	Joyce Meneses	Joyce
07	Rosy Caunder	Rosy
58	Samruddhi Racerone	Ros
46	Alitta Vaeghere	Alitta
36	Desmond hobbs	Desmond
59	Sagar J. Rao	Sagar Rao
70	David Varghese	David
44	Shesha Palamattam	Shesha
56	Priyanka Puarik	Priyanka
48	Karsheda Patil	Karsheda
01	Russel Abreo.	Russel
20	Brijal Dsouza	Brijal
29	Aishwarya Jadhav	Aishwarya
08	SAGAR CHANCHAL	Sagar
39	Rahul Mendes	Rahul
35	Nithu Kumar	Nithu
17	Atthasua Deshmukh	Atthasua
11	Christy Lyona J.V	Christy
28	Jacklin Presella	Jacklin
23	Diana D'Souza	Diana
34	Tooba Khan	Tooba
13	Calvin Crasto	Calvin
76	Sagarika Yadav	Sagarika
51	Alistair Pereira	Alistair
68	Tushar Shinde	Tushar
63	Bryan Sanil	Bryan
19	Olivia D'Sa	Olivia
24	Delvin Davis	Delvin

**DON BOSCO INSTITUTE OF TECHNOLOGY**  
DEPARTMENT OF COMPUTER ENGINEERING

**WORKSHOP ON NETWORK SECURITY APPLICATIONS**  
ATTENDANCE SHEET

CLASS: T.E.      DATE: 22/02/2019  
SUBJECT: CRYPTOGRAPHY AND SYSTEM SECURITY

TIME: 11AM TO 1PM  
VENUE: COMP LAB - 4

ROLL NO	NAME OF STUDENT	SIGNATURE
16	Tanmay Desai	Tanmay
69	Sayel Sajib Mussa	Sayel
42	Padmesh Nair	Pad
49	Yogesh Patil	Yogesh
4	Shivam Baikerikar	Shivam
41	Yash Mishra	Yash
30	Yaidehi Jadhav	Yaidehi
37	Shita Manes	Shita
67	TARUN. SHETTY	Tarun
43	Rohini Nimbekar	Rohini
57	Nikhil Raina	Nikhil
71	Robin Varghese	Robin
55	AKHIL THOMAS	Akhil
03	Elana Alphonso	Elana
22	Denzil Dsouza	Denzil
253	Rahul Krathu	Rahul
25	GIEFFORD FERNANDES	Giefford
61	Juan Rodriguez	Juan Rodriguez
74	Santosh Wadkar	Santosh
06	Dipesh Bharambe	Dipesh
05	Sourab Baskar	Sourab
18	Ram Deshmukh	Ram
27	Clyde Gomes	Clyde
32	Pranav Kale	Pranav
64	Shubham Sapkal	Shubham
10	Mihir Chitre	Mihir
26	Shalomi Fernandes	Shalomi F.
31	Joemol Joy	Joemol