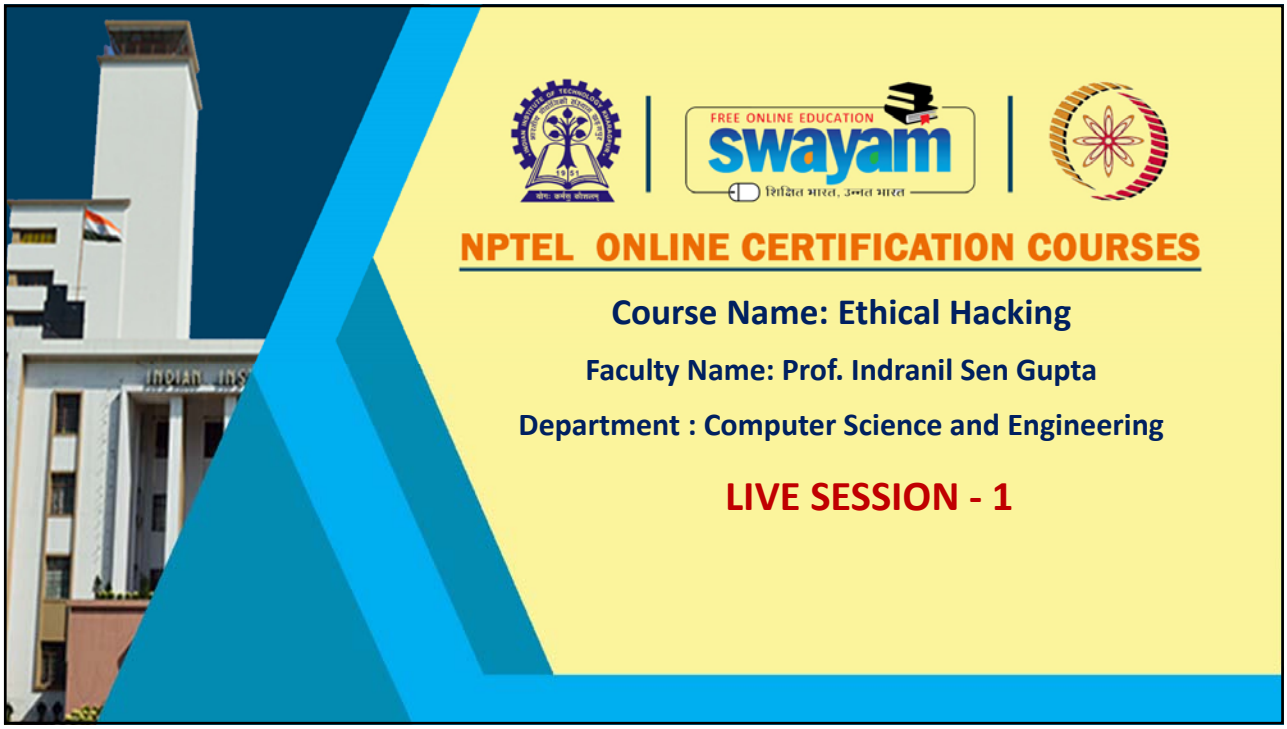

Query 1: **Could you give some explanation of how data in encrypted and decrypted in the TCP/IP layers during transfer of message?**

In normal TCP/IP communication, data are not encrypted. However, there are tools like SSH that provides encryption at the network layer also. In HTTPS, encryption and decryption is handled at the application layer.

Query 2: **In Assignment 6 - Q 3, key length in triple-DES is 168 bits but in question there is "Effective", so effective key length in triple-DES should be 112 bits (As a search result on Google).**

If data packet has triple node encryption, how could it still reveal the data?

Triple-DES uses E-D-E for encryption with keys K1, K2, K3; and D-E-D for decryption with the keys used in reverse order. If K1, K2, K3 are different then the effective key size is 168 bits. However, in many usages of triple-DES, K1 = K3, and the effective key size becomes 112 bits.

An encrypted message can be revealed only if the attacker finds a way to exploit some weakness in the encryption algorithm.


3

All TCP messages (segments) are given to IP for delivery to the final destination in the form of packets. The TCP layer at the final destination checks whether all packets have arrived; if some are missing, an explicit re

Query 4: **What is the meaning of broadcast?**

When a message is sent out to all the hosts in a network, it is called broadcast.

Query 5: **What is difference between ethical hackers and other hackers? What is use and purpose of ethical hackers in companies?**

Ethical hackers mount attacks on network with non-malicious intent.

Ethical hackers try to find out vulnerabilities in a network, so that they can be mitigated.


4

Query 6: **In one way hash function, the message (M) and key (K) are appended together and perform hash function on it and sending to receiver. Why the receiver again need to append key to M? Already it contains "message and key", if we append the key with hashed message then the output hash value will different from sender's hash value?**

The typical flow is like this:

- *The secret key value K is appended to the message M, and hash is computed as H = hash (K || M).*
- *M and H are sent to the receiver, who also knows the secret key K.*
- *The receiver re-computes the hash H' = hash (K || M') based on the received message M'.*
- *Receiver compares H' with the received hash value.*


5

Query 7: **In TCP it provides a reliable data transfer, whereas IP provides unreliable data transfer. Then how we are going to get the reliability of the data transfer?**

All TCP messages (segments) are given to IP for delivery to the final destination in the form of packets. The TCP layer at the final destination checks whether all packets have arrived; if some are missing, an explicit request for retransmission is sent to the sender. In this way, TCP ensures reliability even though the underlying IP is not reliable.


6

Query 8: **Relating to NMAP:**

- **Please explain the all the commands of nmap in details.**
- **While performing nmap for vulnerability scan it doesn't finish and just keeps on scanning even if I use -T4 what is the solution to this?**

Many of the tools like NMAP that are very useful in ethical hacking have not been explained in a formal way, although demonstrations have been given. In the last week, some lectures on these tools shall be provided so that some of the queries you are having can be resolved.

This problem is because the IP is unreachable or it is not finding any open port. To eliminate this, use " - - count<number of rounds>". If you use this then, after scanning each port for an specific number of times, nmap will stop scanning.


7

Query 9: **Difference between Vulnerability Assessment and Security Assessment**

- ***Security assessment****: Should broadly include two components – (a) Security Review:- A collaborative process that includes identifying security issues and their levels of risk, (b) Risk Mitigation:- preparing a plan to mitigate the risks.*
- ***Vulnerability assessment****: It is the testing process used to identify as many security flaws as possible within a given timeframe.*


8

Query 10: **How Trusted Platform Module (TPM) works?**

TPM uses various hardware and software security mechanisms so that it become "almost impossible" to hack. However, there are instances where a TPM chip has been hacked.

We talk about TPM to try and make our systems as secure as possible. Nothing is 100% fool-proof.

9

Query 11: **Regarding job opportunities**

A career in ethical hacking required in-depth knowledge of various fields in computer science and also wide experience in handling tools. There are a number of on-line courses available that can help you to brush up your skills. No course can make you an expert … only hard work and dedication can make it happen.

There are opportunities in large companies who hire people to carry out penetration testing and secure their networks. There are groups of people who have opened start-ups and have been quite successful --- they had to develop a lot of in-house tools in addition to the readily available ones.

Internship opportunities are available to the toppers (top 5%) in each subject.

10

Query 12: **How to identify "clickjacking" in a website?**

This is very difficult to detect. The best way is to analyze the hyperlink that would get activated when the webpage element is clicked.

There are several frame-based techniques to detect whether a web page can be potentially clickjacked (e.g. whether the whole page can be loaded into a frame, etc.)

11

Query 13: **Why is Linux preferred for hacking?**

Linux is an extremely popular operating system for hackers. There are two main reasons behind this.

a) *Linux's source code is freely available because it is an open source operating system. This means that Linux is very easy to modify or customize.*

b) *There are many Linux security distributions available (e.g. Kali) that can double as Linux hacking software.*

12

Query 14: **How do we stay anonymous?**

a) *Browsing in **private mode**. This disables all cookies.*
b) *Be aware that search engines like Google collect information about you.*
c) *Hide your IP address using a **proxy server** or a **Virtual Private Network (VPN).***
d) *Use TOR: It works on the concept of **onion routing** method where the user data is first encrypted and then transferred through different relays present in the Tor network, thus creating a multi-layered encryption (layers like an onion), thereby keeping the identity of the user safe.*

13

Query 15: **Is there any other reliable method of password cracking other than brute forcing?**

There are many sophisticated ways other than brute force technique, like dictionary-based attack, rainbow attack, etc.

Password cracking is considered to be a relatively easy task, as many users tend to use weak passwords.

14

Query 16: **The Nexus vulnerabilities scanner is expensive, how to learn Nexus for free?**

There is a free version of Nexus that you can download and use; of course, it will not come with all the features. But for beginners, the free version should be good enough to get started. (see https://nexus.en.softonic.com/download)


15

Query 17: **Specific applications of TCP and UDP**

UDP applications*: Routing Information Protocol (RIP), Domain Name System (DNS), streaming media applications (IPTV), Dynamic Host Control Protocol (DHCP), Simple Network Management Protocol (SNMP).*

TCP applications*: Electronic mail, FTP, secure shell, HTTP.*


16

Query 18: **Can I do exploitation in two PC's having Ubuntu OS but they are connected to a network using switch?**

Yes you can, but note that when the PCs are connected through a switch, they will belong to different networks.

Query 19: **What is the difference between edge router and default gateway?**

Edge Router*: It is a specialized router residing at the edge or boundary of a network. It ensures connectivity of its network with external networks.*

(also referred to as ***Access Router*** *or* ***Core Router****)*

Default Gateway*: It is the node in a network that serves as the forwarding host (router) to other networks when no other route specification matches the destination IP address of a packet.*

Query 20: **How can data science technologies like deep learning and neural networks be used to make better encryption, hashing algorithms? How can these technologies be used in cybersecurity and cryptography?**

Data science can be used to analyze vulnerabilities in a network, and not for designing algorithms.


19

Query 21: **While using nmap, we were only able to enter in host system if hosts firewalls are down and ports are open, but normally every computer has there firewalls active all the time and there port 80 is mostly closed than why do these computer get viruses?**

There are many ways some virus can affect a system. The most common way is to open a malicious attachment sent over email.


20

Query 22: **How to ping someone on other network, if you have an IP of the network. How does the NAT works?**

The "ping" command can be used, which generates an ICMP packet.

A NAT translates a private address to some public address, and vice versa. It typically uses a technique called Port Address Translation (PAT).


21

Query 23: **How to create a real intrusion attack on any managed device, to check HIDS is working properly or not?**

To check if the host-based IDS (HIDS) is working properly or not, apply some attacks like amplification attack, buffer overflow attack, UDP attack, and ICMP attack.

Then check whether HIDS is able to detect or not. Some of the given attacks will be discussed in week 9.


22

Query 24: **How effectively we can use machine learning algorithms to mount some kind of attacks or to create defences like spam detection in mailing system?**

Some research papers are available that shows that phishing attacks can be determined using machine learning. In this approach some specific words like, win, prizes, lucky winner, and grammar mistakes etc. are considered. For this first you have to provide thousands of spam and non-spam emails. Then your algorithm will identify which are the topmost words that are used in spam mails, and according to that it will mark new mail as spam or not spam. In similar way you can make antivirus and firewall by training with lots of genuine and fake application/packets.


23

Query 25: **Should metasploit be used within a network or outside of a network?**

Metasploit works for both, internal and external network. But you should not perform outside your network without their authorization.


24

SUMMARY

- You are solely responsible for the act you carry out.
  - Ethical hacking is a very tricky subject.
  - Never do anything that can create harm to others.
  - Accessing information without the consent of the owner amounts to stealing.
- Very strong cyber security regulations shall emerge.
- Bottom line: be a responsible and honest citizen.

25

26