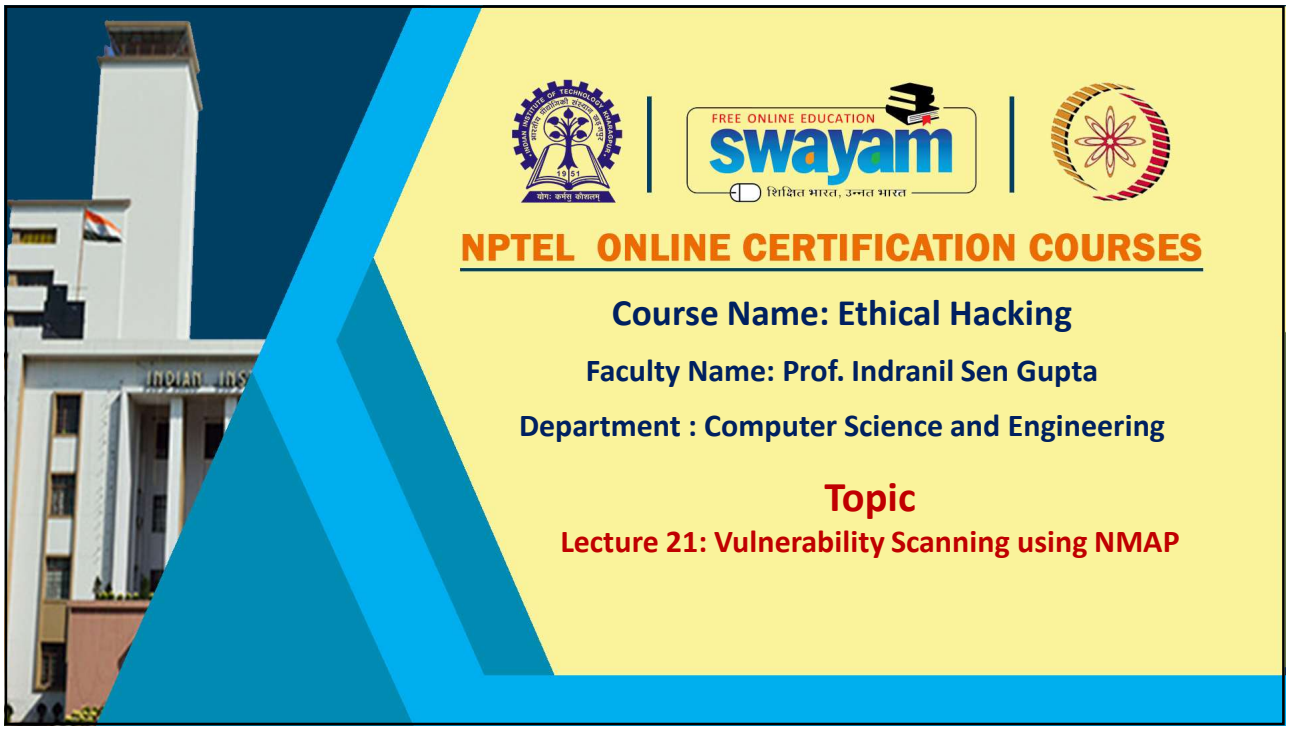
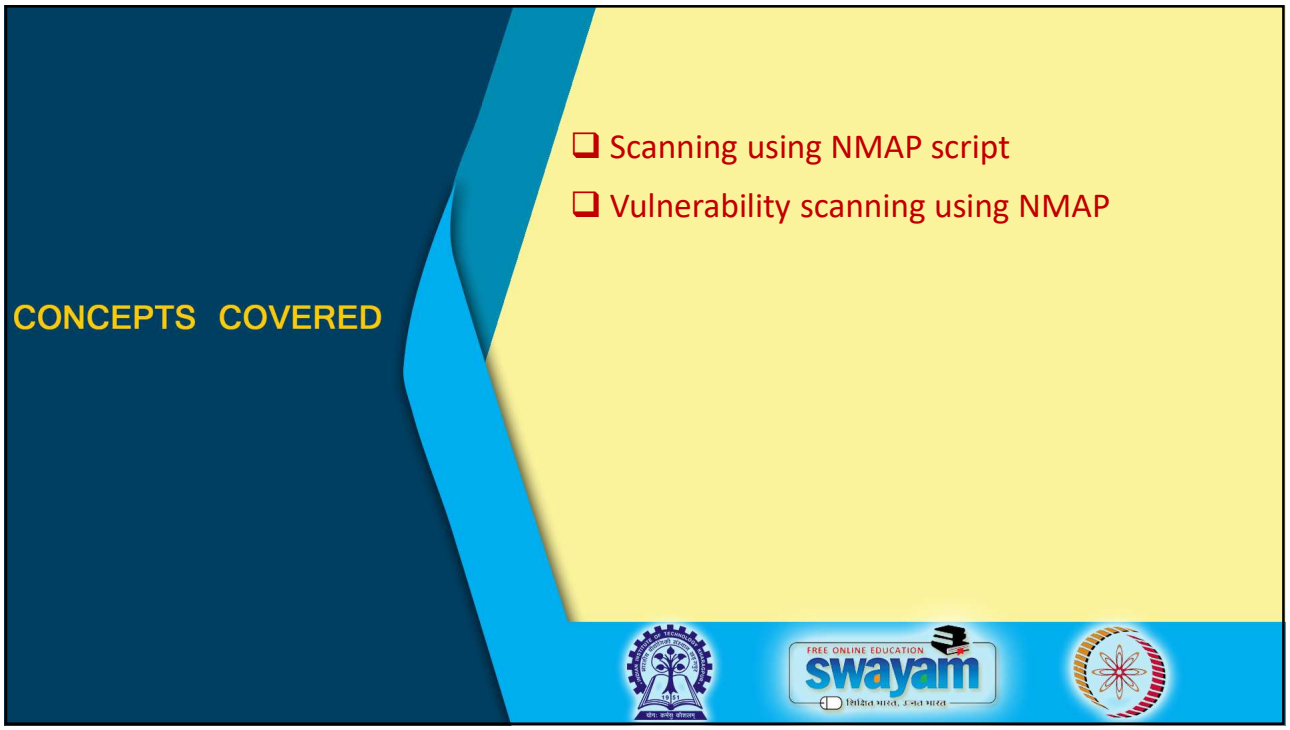

NPTEL ONLINE CERTIFICATION COURSES
Course Name: Ethical Hacking
Faculty Name: Prof. Indranil Sen Gupta
Department : Computer Science and Engineering
Topic
Lecture 21: Vulnerability Scanning using NMAP

NPTEL


CONCEPTS COVERED
Scanning using NMAP script
Vulnerability scanning using NMAP

Scanning Using NMAP Script

- Thousands of scripts available with NMAP to perform various operations.
  - Can have own specific requirements, like some services running, port requirements, etc.
- The detailed guidelines to use NMAP scripts are available with official website: https://nmap.org/book/man-nse.html
- All the scripts related to particular keyword can be obtained as:

```
nmap --script "keyword-*"
```

- Any script can be run using the command:

```
--script <script name> <port # if required> <target>
```

3

NPTEL

Scanning Using NMAP Script (contd.)

- You can find all the scripts by typing the following commands in Kali Linux command prompt:

```
ls -al /usr/share/namap/scripts
```

- The scripts can be useful for automated scanning, vulnerability detection, backdoor detection, port detection, etc.

4

Demonstration: NMAP Scripts

NPTEL

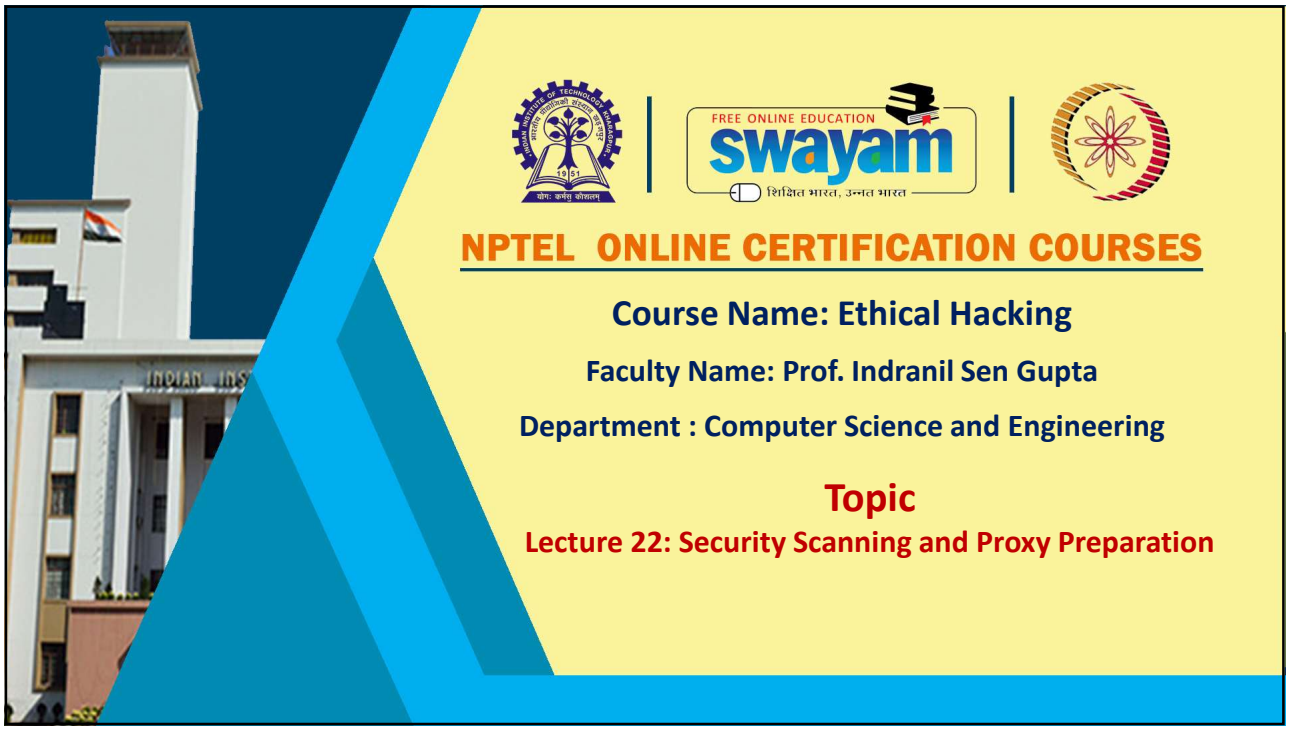
Vulnerability Scanning

- The purpose is to identify vulnerabilities and weaknesses of a system / network in order to determine how a system can be exploited.
- NMAP scripts, Nessus, Nexpose, MBSA, OpenVAS can be used for scanning vulnerability.

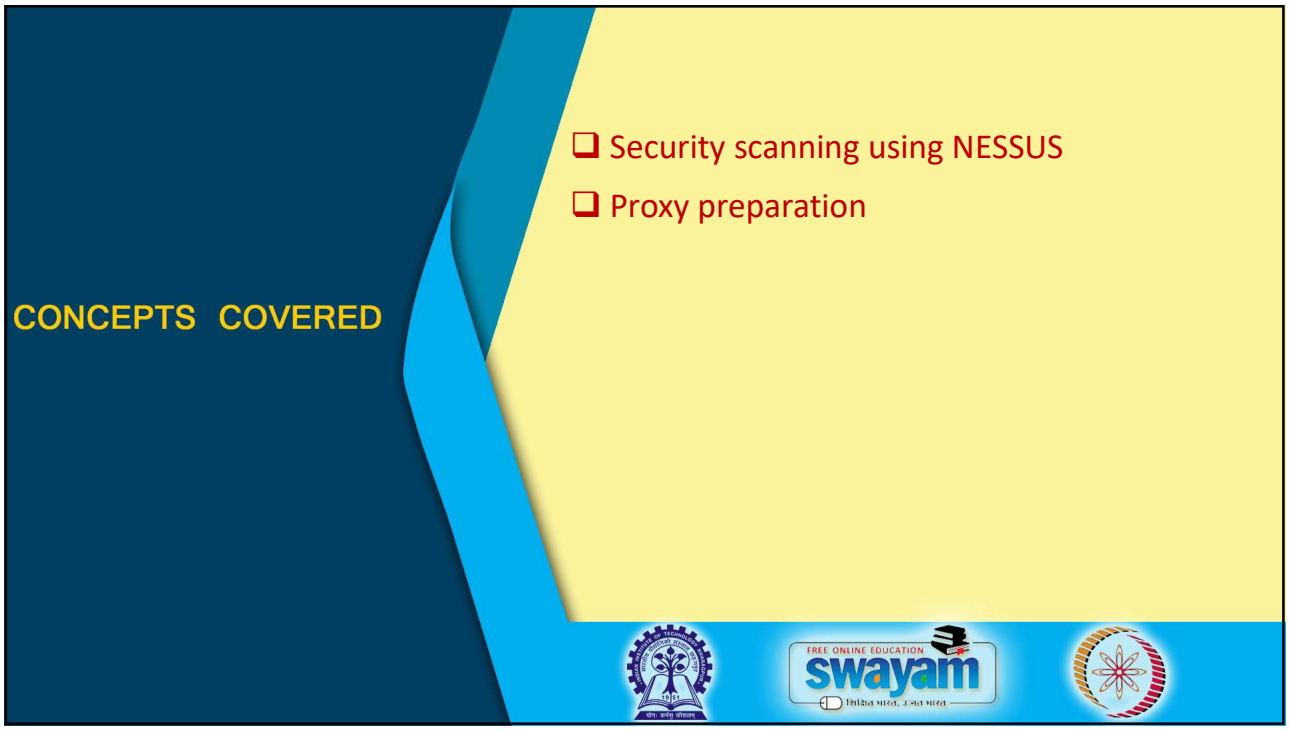
Demonstration: Vulnerability Scanning using NMAP

7

NPTEL


NPTEL ONLINE CERTIFICATION COURSES
Course Name: Ethical Hacking
Faculty Name: Prof. Indranil Sen Gupta
Department : Computer Science and Engineering
Topic
Lecture 22: Security Scanning and Proxy Preparation

NPTEL


CONCEPTS COVERED
Security scanning using NESSUS
Proxy preparation

Vulnerability Scanning using NESSUS

- Nessus is a remote security scanning tool, which scans a computer/network and raise an alert if any vulnerability is discovered.
- It is mostly used by various organizations for vulnerability assessment.
- As compare to NMAP, Nessus is more popular.
  - Free version is not available; we have to purchase the software.
  - We can try free version of Nessus for 7 days.

11

NPTEL

NESSUS (contd.)

- Nessus can be downloaded from: https://www.tenable.com/products/nessus/nessus-professional
- It supports wide variety of scanning options with easy user interface, and produces detailed analysis report of the scan.

12

Demonstration: Vulnerability Scanning using NESSUS

NPTEL

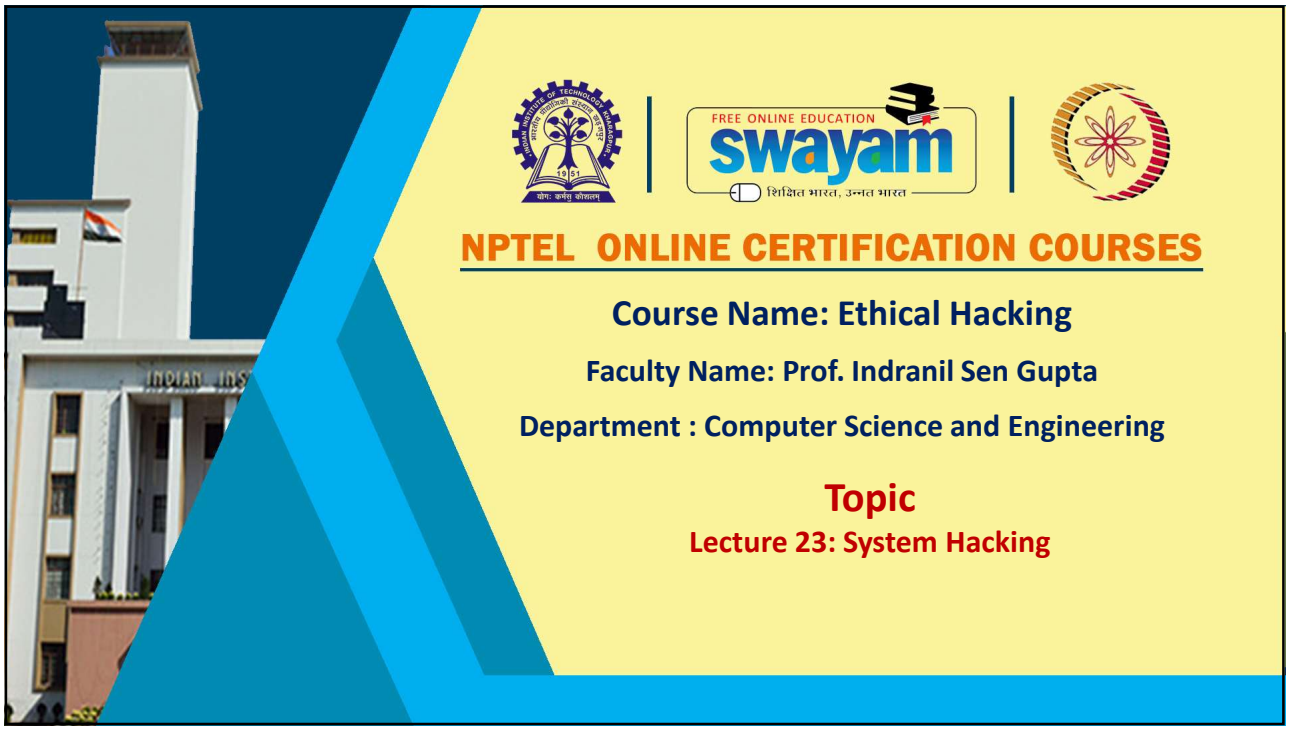
Proxy Preparation

- After collecting all the necessary information for mounting an attack, we also need to prepare proxy such that the attacker is hidden from the victim system.
- Proxy servers can be used for:
  - Work as an intermediary for connecting with victim system.
  - To hide the source IP address so that an attack can be mounted without any legal corollary.
  - To mask the actual source of attack by impersonating a fake source address of the proxy.
- IP spoofing can also be used for the same.
  - We shall look into it later.

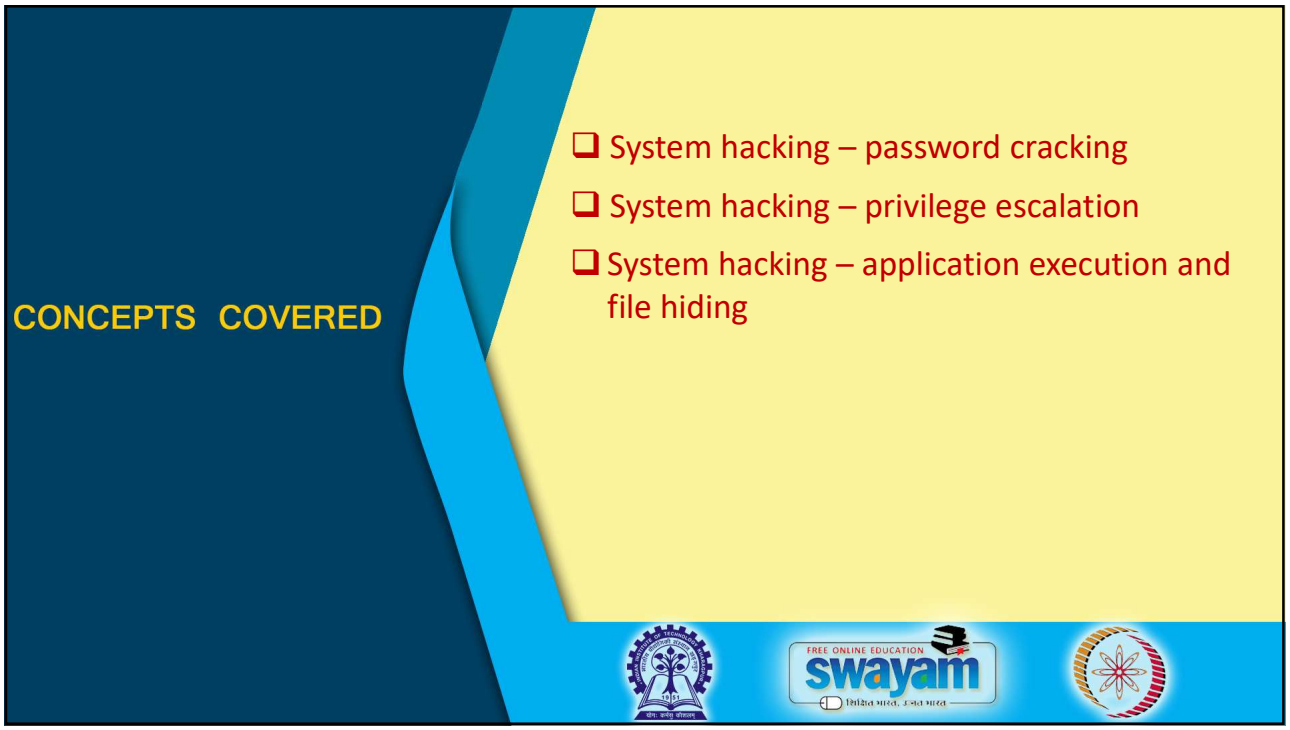
Demonstration: Proxy Preparation

15

NPTEL


NPTEL ONLINE CERTIFICATION COURSES
Course Name: Ethical Hacking
Faculty Name: Prof. Indranil Sen Gupta
Department : Computer Science and Engineering
Topic
Lecture 23: System Hacking

NPTEL


CONCEPTS COVERED
System hacking – password cracking
System hacking – privilege escalation
System hacking – application execution and file hiding

(a) System Hacking: Password Cracking

- System hacking is defined as the compromise of computer systems and software to access a target computer and steal / misuse information stored therein.
- Password cracking
  - Set of techniques used to recover passwords from computer systems.
  - Attackers use this techniques to gain unauthorized access to the vulnerable system.
  - Most of these techniques are successful due to weak or easily guessable passwords.

19

NPTEL

(a) System Hacking: Password Cracking (contd.)

- Some of the well known method of password cracking are:
  - **Shoulder Surfing**: Looking at the user's keyboard or screen while he/she is logging in.
  - **Social Engineering**: Convincing people to reveal passwords.
  - **Dictionary Attack**: A dictionary file is used that runs against user accounts.
  - **Brute-Force Attack**: Try every combination of characters until the password is broken.
  - **Rule-based Attack**: Used when the attacker gets some information about the password.
  - **Password Guessing**: The attacker creates a list of all possible passwords from the information collected through social engineering or any other way, and tries them manually on the victim's machine to crack the passwords.

20

(a) System Hacking: Password Cracking (contd.)

- Some of the well known method for password cracking:
  - **Default Passwords**: Many people do not change default password of manufacturer.
  - **Trojan/Spyware/Keylogger**: Runs in the background, send back all information to attacker.
  - **Wire Sniffing**: Attackers run packet sniffer tools on the local area network (LAN) to access and record the raw network traffic, which may contain user names and passwords.
  - **Rainbow Table**: It is a precomputed table that contains word lists like dictionary files and brute force lists and their hash values.
- Tools used:
  - **john the ripper**, **hydra**, **hashcat**, **crunch**, etc.

21

NPTEL

Demonstration: Password Cracking

22

(b) System Hacking: Privilege Escalation

- An attacker can gain access to the network using a non-admin user account, and the next step would be to gain administrative privileges.
  - Attacker performs privilege escalation attack.
  - Takes advantages of design flaws, programming errors, bugs, and configuration oversights in the OS and software application to gain administrative access to the network.
  - These privileges allows attacker to view critical/sensitive information, delete files, or install malicious programs such as viruses, Trojans, worms, etc.

23

NPTEL

(b) System Hacking: Privilege Escalation

- Types of Privilege Escalation:
  - **Vertical Privilege Escalation**: Refers to gaining higher privileges than existing one.
  - **Horizontal Privilege Escalation**: Refers to acquiring the same level of privileges that already has been granted but assuming the identify of another user with the similar privileges.
- How to Defend against Privilege Escalation?
  - Restrict the interactive logon privileges.
  - Use encryption technique to protect sensitive data.
  - Run user-level applications on the least privileges.
  - Reduce the amount of code that runs with particular privilege.

24

Demonstration: Privilege Escalation

NPTEL

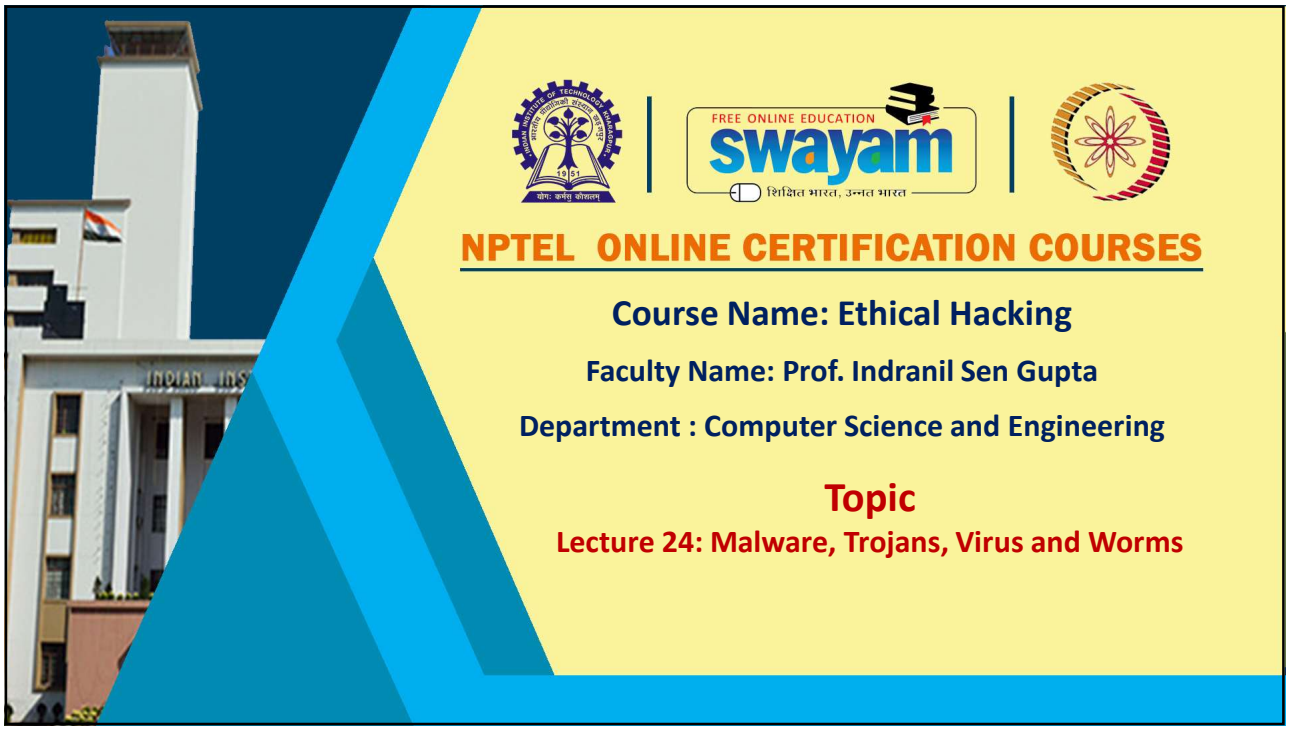
(c) System Hacking: Application Execution and File Hiding

- Once the attacker gets username password or privilege:
  - Executes malicious programs remotely in the victim's machine to gather information that leads to exploitation or loss of privacy, gain unauthorized access to system resources, capture screenshots, install backdoor to maintain easy access, etc.
- Tools used:
  - **PDQ Deploy**: Atool that allows admins to silently install almost any application or patch.
  - **DameWare Remote Support**: Lets you mange servers, notebooks, and laptops remotely.
  - **Keylogger**

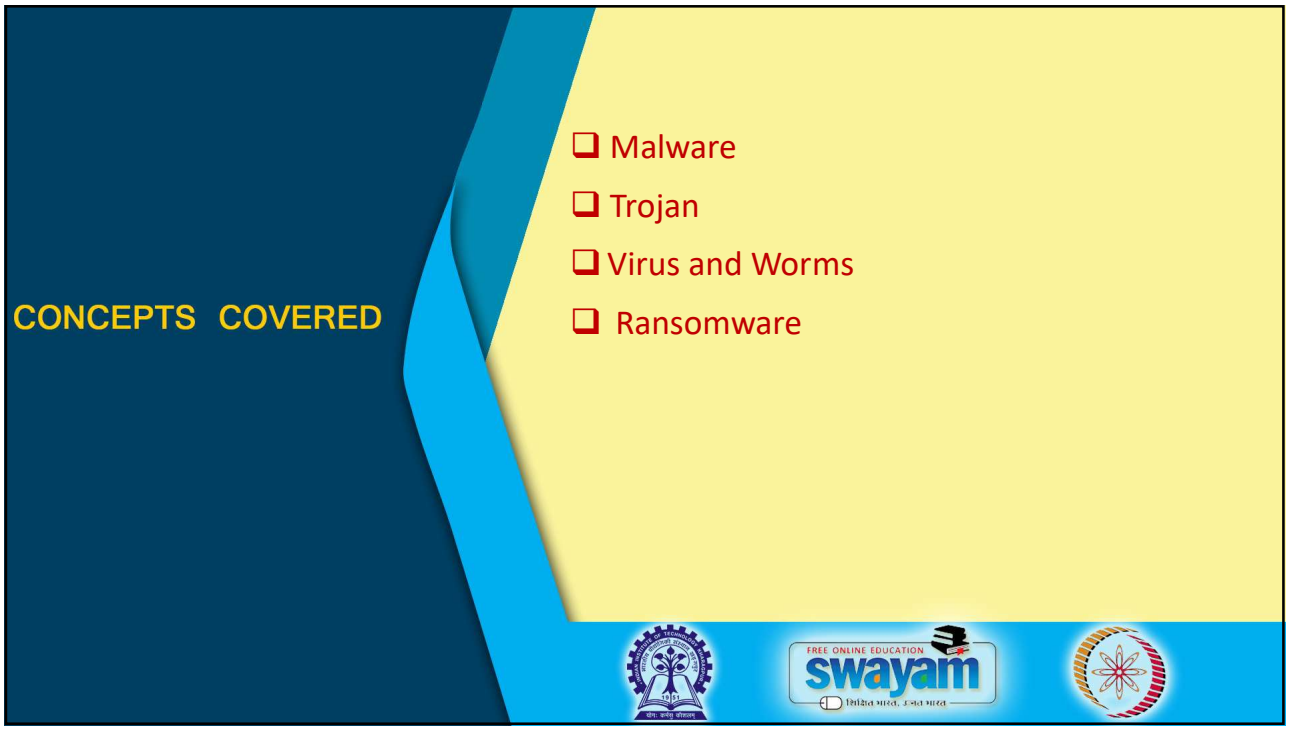
Demonstration: Application Execution

27

NPTEL


NPTEL ONLINE CERTIFICATION COURSES
Course Name: Ethical Hacking
Faculty Name: Prof. Indranil Sen Gupta
Department : Computer Science and Engineering
Topic
Lecture 24: Malware, Trojans, Virus and Worms

NPTEL


CONCEPTS COVERED
Malware
Trojan
Virus and Worms
Ransomware

Malware

- Malicious software that damages or disables computer systems and gives limited or full control to the malware creator for the purpose of theft or fraud.
- Examples of Malware:
  - Trojan Horse and Backdoor
  - Rootkit
  - Ransomware
  - Adware
  - Virus and Worms
  - Spyware
  - Botnet

31

NPTEL

How can Malware get into a system?

- Instant Messenger applications
- IRC (Internet Relay Chat)
- Removable devices
- Attachments
- Browser and email software bugs
- NetBIOS (File Sharing)
- Fake programs
- Untrusted sites and freeware software

32

Trojan

- A program where malicious code is contained inside apparently harmless code or data in such a way that it can get control and cause damage.
- They get activated upon users' certain predefined actions.
- Indications of a Trojan attack include abnormal system and network activities such as disabling of antivirus, redirection to unknown pages, etc.
- Trojans create a covert communication channel between victim computer and attacker for transferring sensitive data.

33

NPTEL

How Hackers use Trojans?

- Delete or replace OS's critical files.
- Generate fake traffic to create DoS attacks.
- Record screenshots, audio, and video of victim's PC.
- Use victim's PC for spamming and blasting email messages.
- Download spyware, adware, and malicious files.
- Disable firewalls and antivirus.
- Create backdoors to gain remote access.
- Infect victim's PC as a proxy server for replaying attacks.
- Use victim's PC as a botnet to perform DDoS attacks.

34

Virus and Worm

- A virus is a self-replicating program that produces its own copy by attaching itself to another program, computer boot sector or document.
  - Generally transmitted through file downloads, infected drives, as email attachments, etc.
- Virus Characteristics:
  - Stages of infecting other program
  - Transforms itself
  - Encrypts itself
  - Alters data
  - Corrupts files and programs

35

NPTEL

Virus and Worm

- **Infection Phase**: The virus replicates itself and attaches to an .exe file.
- **Attack Phase**: Viruses are programmed with trigger events to activate and corrupt systems.
  - Some viruses infect each time they are run, and others infect only when a certain predefined condition is met.
- Type of Virus:
  - Virus hoax
  - Spooky virus
  - Stealth virus
  - Polymorphic virus

36

Ransomware

- It is a type of a malware that restricts access to the computer system's files and folders, and demands an online ransom payment to the malware creator(s) in order to remove the restrictions.
  - Quite common nowadays.

37

NPTEL

Countermeasures against Malwares, Trojans, etc.

- Use of authentic antivirus tool
- Use of firewalls – both personal and organization-level
- Update software on time
- Avoid visiting malicious website
- Do not use obvious passwords
- Ignore unknown mails

38

Demonstration: Malware Scanning, Virus and Trojan

39

NPTEL

Virus

- To test antivirus:

  X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRU-TEST-FILE!$H+H*

- Turn off internet connection

  @Echo off

  Ipconfig /release

- Turn on internet connection

  @Echo off

  Ipconfig /renew

40

Virus

- Popup windows

  X=MsgBox("your text here",num1+num2,“Titel")

- With Loop

  do

  X=MsgBox(“Virus Spreading”, 0+48, “Virus Warning”)

  Loop

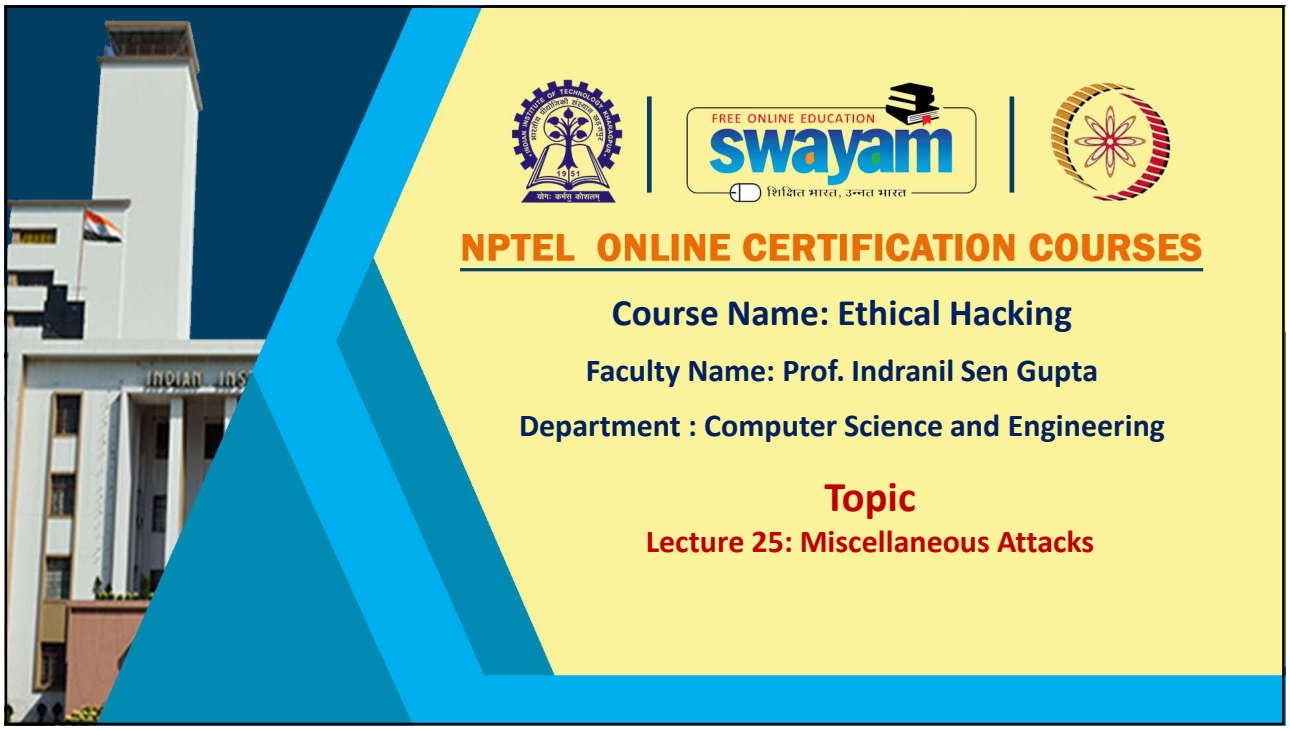
Description for popup windows

num1 is for the type of buttons in the popup
0 = OK Button
1 = OK and Cancel Buttons
2 = Abort, Retry and Ignore Buttons
3 = Yes, No and Cancel Buttons
4 = Yes and No Buttons
5 = Retry and Cancel Buttons

num2 is for the type of icons in the popup
16 = Critical Icon
32 = Help Icon
48 = Warning Icon
64 = Information Icon

41

NPTEL


NPTEL ONLINE CERTIFICATION COURSES
Course Name: Ethical Hacking
Faculty Name: Prof. Indranil Sen Gupta
Department : Computer Science and Engineering
Topic
Lecture 25: Miscellaneous Attacks

NPTEL


CONCEPTS COVERED
Sniffing – principal of operation and types
Various protocol-specific attacks

Packet Sniffing

- It is a process of monitoring and capturing all data packets passing through a given network using sniffing tools.
  - It is a form of wiretap applied to computer networks.
- Many enterprise' switch ports are open.
  - Anyone in the same physical location can plug into the network using an Ethernet cable.

45

NPTEL

How Packet Sniffer works?

- **Promiscuous Mode**: The tool turns the NIC of a system to the promiscuous mode so that it listens to all the data transmitted on its segment.
- **Decode Information**: A sniffer can constantly monitor all the network traffic to a computer through the NIC by decoding the information encapsulated in the data packet.

46

Types of Sniffing:

- **Passive Sniffing**: It means sniffing through a hub, where traffic is sent to all ports. It involves only monitoring of the packets sent by others without sending any additional data packets in the network traffic.
  - In a network that use hubs to connect systems, all hosts can see all traffic -- attacker can easily capture traffic going through the hub.
  - Hub usage is outdated today -- Most modern networks use switches.
- **Active Sniffing**: This is used to sniff a switch-based network.
  - Involves ARP packets into the network to flood the switch's CAM table.
  - CAM keeps track of which host is connected to which port.

47

NPTEL

Vulnerable Protocols

- **HTTP**: Data sent in clear text
- **Telnet and Rlogin**: Keystrokes including user names and passwords
- **POP**: Passwords and data sent in clear text
- **IMAP**: Passwords and data sent in clear text
- **SMTP** and **NNTP**: Passwords and data sent in clear text
- **FTP**: Passwords and data sent in clear text

48

MAC Attack

- Each switch has a fixed size dynamic Content Addressable Memory (CAM) table.
  - The table stores MAC addresses available on ports with their associated VLAN parameters.
  - Once the table on the switch is full, additional ARP request traffic will flood every port on the switch (like a hub).
  - This will change the behavior of the switch to reset to its learning mode.
- This attack will also fill the CAM tables of adjacent switches.
  - MAC Flooding
  - Involves flooding of CAM table with fake MAC address and IP pairs until it is full.

49

NPTEL

DHCP Starvation Attack

- DHCP servers maintain TCP/IP configuration information in a database
  - Valid TCP/IP configuration parameters, IP addresses, duration of lease offered by the server.
- DHCP Starvation Attack:
  - A DoS attack on the DHCP servers where attacker broadcasts forged DHCP requests and tries to lease all of the DHCP addresses available in the DHCP scope.
  - Legitimate user is unable to obtain or renew an IP address requested via DHCP

50

ARP Spoofing

- ARP packets can be forged to send data to the attacker's machine.
- ARP Spoofing involves constructing a large number of forged ARP request and reply packets to overload a switch.
  - Switch is set in "forwarding mode" after ARP table is flooded with spoofed ARP replies and attackers can sniff all the network packets.
  - Attackers flood a target computer's ARP cache with forged entries, which is also known as poisoning.

51

NPTEL

ARP Poisoning

- Using fake ARP messages, an attacker can divert all communications between two machines so that all traffic is exchanged via his/her PC.
- The threats of ARP poisoning include:
  - Packet Sniffing, Session Hijacking, VoIP Call Tapping, Manipulating Data, Man-in-the-Middle Attack, Data Interception, Connection Hijacking and Resetting, Steal Passwords, DoS Attack
- ARP Poisoning Tools:
  - **Cain & Abel** and **WinArpAttacker**

52

Demonstration: ARP Spoofing, MAC Attack

53

NPTEL