

# Cyber Security Intro

- Cyber security is combination of two words CYBER and SECURITY.
  - Cyber means information that is in digital form on Internet and publicly available.
  - Security means we have to provide protection to these data that is available on internet.
- Definition of Cyber Security
  - Practice of protecting systems, networks, programs from Digital or Malicious Attacks.
  - These attacks are usually aim to accessing the information or destroying sensitive information.

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Paste Format Painter New Slide Reset Section Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Shape Fill Shape Outline Quick Styles Shape Effects

Find Replace Select

3 Team Code flfnku7

4 Cyber Security Intro

Cyber security is combination of two words Cyber and Security. Cyber means information that is in digital form on Internet and security means protection of that information. So Cyber security is protection of private information from unauthorized access or interference.

Definition of Cyber Security

Malware, Virus, Trojans, Worms, Ransomware, Rerectors, Programs from Digital or Malicious Attacks.

These attacks are usually done to accessing the information or destroying sensitive information.

5 Virus

A computer virus is a program that can copy itself and infect a computer without the permission or knowledge of the user.

A computer virus has 2 major characteristics:

- The ability to replicate itself.
- The ability to attach itself to another computer file.

6 Warning bells for Virus

- Frequent pop-up windows.
- Mass emails being sent from your email account.
- Fake viruses.
- Unusually slow computer performance.
- Unknown programs that start up when you turn on your computer.
- Unusual activities like password changes.

7 Hacker and Hacking

SLIDE 5 OF 96 ENGLISH (INDIA)

Type here to search

Click to add notes

Unit 1 Nishant Doshi

NOTES COMMENTS

# Virus



Unit 1.pptx - PowerPoint

Aashka R

FILE HOME DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy New Slide Section Paste Format Painter Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Shape Fill Shape Outline Quick Styles Shape Effects Select

Find Replace

3 Team Code flfnku7

4 Cyber Security Intro

Cyber security is combination of two words CYBER and SECURITY.

- Cyber means information that is in digital form or can be stored in digital form.
- Security means we have to provide protection to these data that is available on internet.

Definition of Cyber Security:

- Practice of protecting systems, networks, programs from Digital or Malicious Attacks.
- These attacks can cause loss of privacy or loss of information or destroying sensitive information.

5 Virus

A computer virus is a program that copies itself and infects a computer without the permission or knowledge of the user.

- A computer virus has 2 major characteristics:
  - The ability to replicate itself.
  - The ability to attack itself to another computer file.

6 Warning bells for Virus

- Frequent pop-up windows.
- Mass emails being sent from your email account.
- Frequent crashes.
- Unusually slow computer performance.
- Unknown programs that start up when you turn on your computer.
- Unusual activities like password changes.

Click to add notes

Unit 1 Nishant Doshi

7 Hacker and Hacking

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste Clipboard Slides Layout New Slide Reset Section

B I U Aa A Text Direction Align Text Convert to SmartArt

Font Paragraph

Shape Fill Shape Outline Quick Styles Shape Effects

Find Replace Select

Editing

5 Virus

A computer virus is a program that can copy itself and spread from one computer to another without the permission or knowledge of the user.

Characteristics:

- The ability to reproduce itself.
- The ability to attach itself to another computer file.

6 Warning bells for Virus

- Frequent pop-up windows.
- Mass emails being sent from your email account.
- Frequent crashes.
- Unusually slow computer performance.
- Unknown programs that start up when you turn on your computer.
- Unusual activities like password changes.

7 Hacker and Hacking

- **HACKING** is the gaining of access to a computer and viewing, copying or creating data without the intention of destroying data or maliciously harming the computer.
- **A hacker is a person skilled in information technology who uses their technical knowledge to achieve a goal or overcome an obstacle, within a computerized system by non-standard means.**
- Someone who utilizes their technical know-how of **bugs or exploits** to break into computer systems and access data which would otherwise be unavailable to them.

8 Types of Hackers

- There are three types of hacker:
  - White Hat Hacker: It involves performing a security audit and testing to gain complex knowledge of the network infrastructure.
  - Gray Hat Hacker: It involves pen testing a security vulnerability to gain access to data.
  - Black Hat Hacker: Testing with no prior knowledge of the network infrastructure or systems.

9 Types of Hacking

Unit 1 Nishant Doshi

Click to add notes

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste New Slide Section Reset Layout Clipboard Slides

Font Paragraph Drawing Editing

Find Replace Select

5 Virus

- A computer virus is a program that can copy itself and infect a temporary or permanent file.
- Without the permission or knowledge of the user.
- A computer virus has 2 major characteristics:
  - The ability to replicate itself.
  - The ability to attach itself to another computer file.

6 Warning bells for Virus

- Frequent pop-up windows.
- Mass emails being sent from your email account.
- Frequent crashes.
- Unusually slow computer performance.
- Unknown programs that start up when you turn on your computer.
- Unusual activities like password changes.

7 Hacker and Hacking

HACKING is the practice of gaining access to a computer system, computer or creating data without the intention of destroying data or maliciously tampering the computer.

• White Hat Hackers: They are ethical hackers who try to find security holes in systems to fix them before they can be exploited by others. Within a compromised system, they assess damage and determine what would allow for the vulnerability to them.

8 Types of Hackers

- There are three types of hacker:
  - White hat hacker: It involves performing a security evaluation and testing with complete knowledge of the network infrastructure.
  - Gray hat Hacker: It involves performing a security evaluation and testing internally.
    - It examines the extent of access by insiders within the network.
  - Black hat Hacker: Testing with no prior knowledge of the network infrastructure or systems.
    - It takes longest amount of time and most efforts.

Unit 1 Nishant Doshi

Click to add notes

NOTES COMMENTS

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy New Slide Section Reset Format Painter Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Shape Fill Shape Outline Quick Styles Shape Effects

Find Replace Select

**Hacker and Hacking**

- HACKING is the action of access or a computer and usually, consists of different ways where the hacker can compromise the system.
- A hacker is a person skilled in information technology who is able to break into a computer system or network without permission.
- Similarly, there are three kinds of hackers who try to break into computers to steal and misuse data which is stored there for their own benefit.

**Types of Hackers**

- There are three types of hacker:
  - White Hat Hacker: It involves performing a security evaluation and testing with complete knowledge of the system's architecture.
  - Grey Hat Hacker: It involves performing a security evaluation and testing internally.
  - Black Hat Hacker: Hacking with no prior knowledge of the network architecture or systems.
  - \* Takes control of the system without permission.

**Types of Hacking**

- **Website Hacking:** Web hacking refers to exploitation of applications via HTTP which can be done by manipulating the application via its graphical web interface, tampering the Uniform Resource Identifier (URI) or tampering HTTP elements not contained in the URI.



Unit 1 Nishant Doshi

Click to add notes

9

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste Clipboard Slides

Layout Reset New Section Slide Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Shape Fill Shape Outline Quick Styles Shape Effects

Arrange Select

9 Types of Hacking

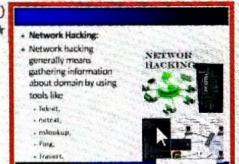
- Website Hacking: Web hacking refers to the exploitation of application vulnerabilities which can be done by manipulating the application via its graphical web interface, tampering the Uniform Resource Identifier (URI) or tampering HTTP elements not contained in the URI.



10 Network Hacking

- Network Hacking: Network hacking generally means gathering information about domain by using tools like

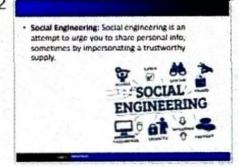
  - Telnet,
  - netcat,
  - nslookup,
  - Ping,
  - Tracert.



11 Password Hacking: Hackers will get your credentials through the keylogging.



12 Social Engineering: Social engineering is an attempt to urge you to share personal info, sometimes by impersonating a trustworthy supply.



# Click to add title

- Network Hacking:**
- Network hacking generally means gathering information about domain by using tools like
  - Telnet,
  - netcat,
  - nslookup,
  - Ping,
  - Tracert.

## NETWOR HACKING



Unit 1 Nishant Doshi

Click to add notes

10

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Shape Fill Shape Outline Quick Styles Shape Effects

Find Replace Select

9 Types of Hacking

- Website Hacking: Web Hacking refers to exploitation of applications via HTTP which can be done by manipulating the application via its graphical web interface or the Uniform Resource Identifier (URI) or tampering HTTP elements not contained in the URL.

10 Network Hacking

- Network hacking generally means gathering information about domain by using tools like
  - Telnet,
  - nmap,
  - enum4l,
  - Cain,
  - Fuzzy.

11 Password Hacking: Hackers will get your credentials through the key-logging.

12 Social Engineering

- Social Engineering: Social engineering is an attempt to urge you to share personal info, sometimes by impersonating a trustworthy supply.

13

Click to add title

• **Password Hacking:** Hackers will get your credentials through the key-logging.

Unit 1 Nishant Doshi

11

Click to add notes

Unit 1.pptx - PowerPoint

Aashka R

LE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Clipboard Slides

Font Paragraph

Drawing Editing

Find Replace Select

Types of Hacking

- Website Hacking: Web hacking refers to manipulation of web services via HTTP which can be done by manipulating the application via its graphical web interface, tampering the Uniform Resource Identifier (URI) or tampering HTTP elements not contained in the URI.

Network Hacking

- Network hacking generally means gathering information about domain by using tools like

  - Nmap
  - Metasploit
  - Nessus
  - Fuzzy
  - Traceroute

1 ★

1 • Password Hacking: Hackers will get your credentials through key-logging.

12

13

Click to add title

- **Social Engineering:** Social engineering is an attempt to urge you to share personal info, sometimes by impersonating a trustworthy supply.

Unit 1 Nishant Doshi

Click to add notes

NOTES COMMENTS

85%

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Shapes Quick Styles Shape Effects

Find Replace Select

12

Social Engineering: Social engineering is an attempt to urge you to share personal info, sometimes by impersonating a trustworthy supply.

SOCIAL ENGINEERING

13

Phishing: In this type of hacking, hackers intention to stole critical information of users like account passwords, MasterCard detail, etc. For example, hackers can make a replicating first website for users interaction and can steal critical information.

14

Malware

Malware is intrusive software that is designed to damage and destroy computers and computer systems. Malware is a contraction for "malicious software."

Mainly designed to transmit information about your web browsing habits to the third party.

15

Malware (Contd.)

Types:

- Viruses
- Trojan Horse
- Spyware
- Adware
- Worms

Click to add title

- **Phishing:** In this type of hacking, hackers intention to stole critical information of users like account passwords, MasterCard detail, etc. For example, hackers can make a replicating first website for users interaction and can steal critical information.

Phishing

Click to add notes

Unit 1 Nishant Doshi

NOTES COMMENTS

Unit 1.pptx - PowerPoint

Aashka R -

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Paste

Clipboard Slides Font Paragraph Drawing Editing

13

14

15

# Malware

- Malware is intrusive software that is designed to damage and destroy computers and computer systems. Malware is a contraction for “malicious software.”
- Mainly designed to transmit information about your web browsing habits to the third party.

Unit 1 Nishant Doshi

Click to add notes

The screenshot shows a Microsoft PowerPoint slide titled "Malware". The slide has a blue header bar with the title. Below the title is a bulleted list:

- Malware is intrusive software that is designed to damage and destroy computers and computer systems. Malware is a contraction for “malicious software.”
- Mainly designed to transmit information about your web browsing habits to the third party.

At the bottom of the slide, there is a footer bar with the text "Unit 1 Nishant Doshi". To the left of the main slide, there are thumbnails of other slides in the presentation, including one about "SOCIAL ENGINEERING" and another about "Malware (Contd.)". The overall interface is that of the Microsoft Office PowerPoint application.

Unit 1.pptx - PowerPoint

Aashka R.

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Layout Reset

Clipboard Slides

SOCIAL ENGINEERING

13

Phishing: In this type of hacking, Hackers intend to stole critical information from users like account password, Microsoft sheets etc. For example, Hackers can make a replicating first website for users interaction and can steal critical information.

14 Malware

Malware is intrusive software that is designed to damage and destroy computers and computer systems. Malware is a contraction for "malicious software". Mainly designed to transmit information about your web browsing habits to the third party.

15 Malware (Contd.)

Types:

- Viruses
- Trojan Horse
- Spyware
- Adware
- Worms

16 INTERNET GOVERNANCE

WSIS FORUM 2023

Click to add notes

Unit 1 Nishant Doshi

NOTES COMMENTS

SLIDE 15 OF 96 ENGLISH (INDIA)

Type here to search

13:36 09-02-2024

# Malware (Contd.)

**Types:**

- Viruses
- Trojan Horse
- Spyware
- Adware
- Worms



15

Malware (Contd.)

- Types:
  - Viruses
  - Trojan Horse
  - Spyware
  - Adware
  - Worms

16 INTERNET GOVERNANCE

WSIS FORUM 2023

17 INTERNET GOVERNANCE

Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet.

18 INTERNET GOVERNANCE

In other word Internet is decentralized network of computers which are connected to each other and runs the internet. And to run internet we have to set some rules.

ARIN is one of the components which eventually control Internet of Internet.

INTERNET GOVERNANCE

19 SELF REGULATION

Self regulation works in a group with strong

Unit 1.pptx - PowerPoint

INTERNET GOVERNANCE

Internet governance is the development and application by

- Governments,
- the private sector and
- civil society,
- in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet.

CURTAIN RAISER  
India Internet Governance  
(Supported by Stakeholder Community)

Rajeev Chandrasekhar, Minister of State, Electronics & Information Technology.

Unit 1 Nishant Doshi

Aashka R

Unit 1.pptx - PowerPoint

Aashka R

**INTERNET GOVERNANCE**

- In other word, Internet is decentralized network of computers. No one, company, government or organization runs the internet. And to run internet we have to set some rules.
- ARPANET is one of the components which eventually evolved to become the Internet.

The diagram illustrates the growth of the Internet from its origins in ARPANET. It shows a small network of four nodes connected by lines, labeled 'ARPANET'. This network then grows into a larger, more complex structure with additional nodes and lines, representing the evolution of the Internet. Labels include 'INTERNET GOVERNANCE', 'WSIS FORUM 2023', 'INTERNET GOVERNANCE', 'INTERNET GOVERNANCE', 'SELF REGULATION', and 'NOTES'.

Unit 1 Nishant Doshi

Click to add notes

19 SELF REGULATION

SIDE 18 OF 96 ENGLISH (INDIA)

13:37 09-02-2024 85%

# SELF REGULATION

- Self regulation works in a group with strong community ties, by applying peer pressure or exclusion.
- ISPs try to self regulate by imposing standards of behavior for their customers.
- Self regulation doesn't always work like IoT where things are managed automatically.

Unit 1.pptx - PowerPoint

Aashka R.

HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

INTERNET GOVERNANCE

In other word Internet is decentralized network of networks which is run by no one. So we have to set some rules to run it. ARIN/ICANN is one of the companies which eventually controls the Internet.

SELF REGULATION

- Self regulation works in a group with strong community ties, by applying peer pressure or exclusion.
- Companies self regulate by imposing standards of behavior for their customers.
- Self regulation doesn't always work like IoT where things are managed automatically.

Policy Making

- Promote the open, distributed and interconnected nature of the Internet.
- Ensure transparency, fair process, and accountability.

CHALLENGES AND CONSTRAINTS

- Ransomware Evolution: Ransomware is a type of malware in which the data on a victim's computer is locked and payment is demanded before the recovered data is released.
- Blockchain Revolution: A Blockchain is a database that stores data in the form of chained blocks.
- IoT Threats: IoT stands for Internet of Things. It is a system of interconnected physical devices which

Unit 1 Nishant Doshi

Click to add notes

NOTES COMMENTS

Unit 1.pptx - PowerPoint

Aashka R.

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Find Replace Select

19 SELF REGULATION

- Self regulation works in a group with strong community ties, by applying peer pressure or inclusion.
- IFPs try to self regulate by imposing standards of behavior for their customers.
- Self regulation doesn't always work like IoT where things are managed automatically.

20 Policy Making

- Promote the open, distributed and interconnected nature of the Internet.
- Ensure transparency, fair process, and accountability.

21 CHALLENGES AND CONSTRAINTS

- Ransomware Evolution: Ransomware is a type of malware in which the data on a victim's computer is locked, and payment is demanded before the ransomed data is unlocked.
- Blockchain Revolution: A blockchain is a database that stores data in the form of chained blocks.
- IoT Threats: IoT stands for Internet of Things. It is a system of interrelated physical devices which can be accessible through the internet.

22 CHALLENGES AND CONSTRAINTS (Contd.)

- AI Expansion: It is an area of computer science which is the creation of intelligent machines that do work and react like humans. Some of the applications of AI include self-driving cars, speech recognition, Learning, Planning, Problem-solving, etc.
- Serverless Apps Vulnerability: Serverless architecture and apps is an application which deploys code directly to cloud infrastructure or on a back end service such as google cloud function, Amazon web services (AWS) lambda, etc.

23 CYBER WARFARE

Click to add notes

Unit 1 Nishant Doshi

NOTES COMMENTS

Unit 1.pptx - PowerPoint

Ashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

Policy Making

- Promote the open, distributed and interconnected nature of the Internet.
- Ensure transparency, fair process, and accountability.

CHALLENGES AND CONSTRAINTS

- Ransomware Ransomware is a type of malware in which the data on a victim's computer is locked, and payment is demanded before the ransomed data is released.
- Blockchain Blockchain is a database that stores data in the form of chained blocks.
- IoT Threats IoT stands for Internet of Things. It is a system of interconnected physical devices which can be accessible through the internet.

CHALLENGES AND CONSTRAINTS (Contd.)

- AI Expansion:** It is an area of computer science which is the creation of intelligent machines that do work and react like humans. Some of the activities related to artificial intelligence include Speech Recognition, Learning, Planning, Problem-solving, etc.
- Serverless Apps Vulnerability:** Serverless architecture and apps is an application which depends on third-party cloud infrastructure or on a back-end service such as google cloud function, Amazon web services (AWS) lambda, etc.

CHALLENGES AND CONSTRAINTS (Contd.)

CHALLENGES AND CONSTRAINTS

- AI Expansion: It is an area of computer science which is the creation of intelligent machines that do work and react like humans. Some of the activities related to artificial intelligence include Speech Recognition, Learning, Planning, Problem-solving, etc.
- Serverless Apps: Serverless architecture and apps is an application which depends on third-party cloud infrastructure or on a back-end service such as google cloud function, Amazon web services (AWS) lambda, etc.

CYBER WARFARE

- Cyber Warfare is internet based conflict involving politically motivated attacks on information systems.
- It also involves the action by a nation-state or International organization to attack and attempt to damage another nation's computers and information.

Click to add notes

Unit 1 Nishant Doshi

NOTES COMMENTS

# CYBER WARFARE

- Cyber Warfare is Internet based conflict involving politically motivated attacks on information systems.
- It also involves the action by a nation-state or International organization to attack and attempt to damage another nation's computers and information.



Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

COPY PASTE CUT FORMAT PAINTER NEW SLIDE SECTION CLIPBOARD SLIDES

Font Paragraph Drawing Editing

CHALLENGES AND CONSTRAINTS (Contd.)

- AI Expansion: It is an area of computer science which is the creation of intelligent machines that do work and react like humans. Some of the applications include natural language processing, speech recognition, learning, planning, problem solving, etc.
- Serverless Apps Vulnerability: Serverless architecture and apps can be attacked which depends on the fact that the infrastructure is on a back end service such as google cloud functions, Amazon web services (AWS) Lambda, etc.

23 CYBER WARFARE

- Cyber Warfare: Internet based conflict involving politically motivated attacks on information systems.
- It also involves the action by a nation-state or international organization to attack and attempt to damage another nation's computers and information.

24 CYBER WARFARE Types

- 1) Espionage
- 2) Sabotage
- 3) DoS Attack
- 4) Electrical Power Grid
- 5) Propaganda Attacks
- 6) Economic Disruption
- 7) Sunrise Attack

25 Espionage

- Refers to monitoring other countries to steal secrets.

26 Sabotage

Unit 1 Nishant Doshi

Click to add notes

NOTES COMMENTS

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

CYBER WARFARE Types

- 1) Espionage
- 2) Sabotage
- 3) Denial Attack
- 4) Electrical Power Grid
- 5) Propaganda Attacks
- 6) Information Disruption
- 7) Counter Attack

25 Espionage

- Refers to monitoring other countries to steal secrets.

Types of industrial espionage

- IP theft
- Property trespass
- Hiring away employees
- Wiretapping or eavesdropping
- Cyber attacks and malware

26 Sabotage

- Government organizations must determine sensitive information and the risks if it is compromised.
- Hostile governments or terrorists may steal information, destroy it, or leverage insider threats such as disloyal or careless employees, or government employees with affiliation to the attacking country.

27 Sabotage (Contd.)



Click to add notes

Unit 1 Nishant Doshi

28 Denial of Service (DoS)

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste New Slide Section Layout Reset

Clipboard Slides

Font Paragraph

Drawing Editing

Find Replace Select

24 CYBER WARFARE Types

1 Espionage  
2 Sabotage  
3 Denial Attack  
4 Electrical Power Grid  
5 Proprietary Assets  
6 Economic Disruption  
7 Terrorist Attack

25 Espionage

Refers to monitoring other countries to steal secrets.

Types of Espionage

26 Sabotage

Government organizations must determine sensitive information and the risks if it is compromised.  
Hostile governments or terrorists may steal information, destroy it, or leverage insider threats such as dissatisfied or careless employees, or government employees with affiliation to the attacking country.

Sabotage (Contd.)

Denial of Service (DoS)

Click to add notes

Unit 1 Nishant Doshi

NOTES COMMENTS

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

CYBER WARFARE Types

- 1) Espionage
- 2) Sabotage
- 3) Den Attack
- 4) Electrical Power Grid
- 5) Propaganda Attacks
- 6) Economic Disruption
- 7) Sunrise Attack

25 Espionage

- Refers to monitoring other countries to steal secrets.

Types of Espionage



26 Sabotage

- Government organizations must determine sensitive information and the risks if it is stolen.
- Hostile governments or terrorists may steal information, destroy it, or leverage insider threats such as disloyal or careless employees, or government employees with affiliation to the attacking country.

27 Sabotage (Contd.)



Click to add notes

28 Denial of Service (DoS)

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Slides

Clipboard

Font Paragraph

Drawing Editing

Find Replace Select

# Denial of Service (DoS)

• DoS attacks prevent legitimate users from accessing a website by flooding it with fake requests and forcing the website to handle these requests.

Sabotage

- Government organizations must determine sensitive information and the risks if it is compromised.
- Hostile governments or terrorists may steal sensitive information or launch cyber threats such as disgruntled or careerless employees, or government employees with affiliation to the attacking country.

Sabotage (Contd.)

Denial of Service (DoS)

- DoS attacks prevent legitimate users from accessing a website by flooding it with fake requests and forcing the website to handle these requests.

Unit 1 Nishant Doshi

Click to add notes

26

27

28

29

Unit 1.pptx - PowerPoint

Aashka R.

HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter

Layout New Slide Section

Clipboard employees, or government employees with affiliation to the attacking country.

Sabotage (Contd.)

Denial of Service (DoS)

- DoS attacks prevent legitimate users from accessing a website by flooding it with fake requests and forcing the website to handle these requests.

Denial of Service (DoS) Attack

Electrical Power Grid

- Attacking the power grid allows attackers to disable critical systems, disrupt infrastructure, and potentially result in bodily harm. Attacks on the power grid can also disrupt communications and render services such as text messages and communications unusable.

Click to add notes

Unit 1 Nishant Doshi

Unit 1.pptx - PowerPoint

Aashka R -

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Paste Format Painter New Slide Section Reset

Clipboard Slides

Font

Text Direction Align Text Convert to SmartArt

Paragraph

Shape Fill Shape Outline Quick Styles Shape Effects

Arrange Find Replace Select

Editing

29

Electrical Power Grid

- Attacking the power grid allows attackers to disable critical systems, disrupt infrastructure, and potentially result in bodily harm. Attacks on the power grid can also disrupt communications and render services such as text messages and communications unusable.

30 Electrical Power Grid

- Attacking the power grid allows attackers to disable critical systems, disrupt infrastructure, and potentially result in bodily harm. Attacks on the power grid can also disrupt communications and render services such as text messages and communications unusable.

31 Electrical Power Grid (Contd.)

32 Propaganda Attacks

- Attempts to control the minds and thoughts of people living in or fighting for a target country

Click to add notes

Unit 1 Nishant Doshi

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste New Slide Section Layout Reset Convert to SmartArt

Clipboard Slides

Font Paragraph Drawing Editing

32 Propaganda Attacks

• Attempts to control the minds and thoughts of people living in or fighting for a target country

31 Electrical Power Grid (Contd.)

YOU HAVE BEEN HACKED !

30 Electrical Power Grid

• Attacking the power grid allows attackers to disable critical systems, disrupt infrastructure, and potentially result in bodily harm. Attacks on the power grid can also disrupt communications and render services such as text messages and communications unusable.

32 Click to add notes

The screenshot shows a Microsoft PowerPoint slide titled "Electrical Power Grid (Contd.)". The slide contains a background image of a power grid at sunset with several transmission towers. Overlaid on the bottom right is a black rectangular box containing the text "YOU HAVE BEEN HACKED !" in green. The slide is part of a larger deck with other slides visible on the left side of the interface.

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Shape Fill Shape Outline Quick Styles Shape Effects

Find Replace Select

32 Propaganda Attacks

• Attempts to control the minds and thoughts of people living in or fighting for a target country

33 Propaganda Attacks (Contd.)

34 Economic Disruption

- Most modern economic systems operate using computers.
- Attacks can target computer networks of economic establishments such as stock markets, payment systems, and banks to steal money or block people from accessing the funds they need.

Source Attack

Click to add notes

Unit 1 Nishant Doshi

NOTES COMMENTS

85%

The screenshot shows a Microsoft PowerPoint slide titled "Propaganda Attacks". The slide contains a single bullet point: "Attempts to control the minds and thoughts of people living in or fighting for a target country". The navigation pane on the left lists other slides: "Propaganda Attacks" (slide 32), "Propaganda Attacks (Contd.)" (slide 33), "Economic Disruption" (slide 34), and "Source Attack". The ribbon at the top includes tabs for FILE, HOME, INSERT, DESIGN, TRANSITIONS, ANIMATIONS, SLIDE SHOW, REVIEW, and VIEW. The HOME tab is selected. The ribbon also features various font and paragraph styles, drawing tools, and editing options. The status bar at the bottom right shows "NOTES" and "COMMENTS" with a red arrow icon, and the page number "85%".

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

33 Propaganda Attacks (Contd.)

34 Economic Disruption

- Most modern economic systems operate using computers.
- Attackers can target computer networks of economic establishments such as stock markets, payment systems, and banks to steal money or block people from accessing the funds they need.

35 Sunrise Attacks

- These are the cyber equivalent of attacks like Pearl Harbor and 9/11.
- The point is to carry out a massive attack that the enemy isn't expecting, enabling the attacker to weaken their defenses.

36 Cybercrime

- Cybercrime is a crime that involves a computer and a network.
- The computer may have been used in the commission of a crime, or it may be the target. Cybercrime may harm someone's security and financial health.

## Propaganda Attacks (Contd.)



Click to add notes

Unit 1.pptx - PowerPoint

Aashka R.

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste New Slide Section Clipboard Slides Font Paragraph Drawing Editing

# Economic Disruption

33 Propaganda Attacks (Contd.)



34 Economic Disruption

- Most modern economic systems operate using computers.
- Attackers can target computer networks of economic establishments such as stock markets, payment systems, and banks to steal money or block people from accessing the funds they need.

35 Sunrise Attacks

- These are the cyber equivalent of attacks like Pearl Harbor and 9/11.
- The point is to carry out a massive attack that the enemy isn't expecting, enabling the attacker to weaken their defenses.

36 Cybercrime

- Cybercrime is a crime that involves a computer and a network.
- The computer may have been used in the commission of a crime, or it may be the target. Cybercrime may harm someone's security and financial health.

Click to add notes

Unit 1 Nishant Doshi

NOTES DOCUMENTS

UNIT 1.pptx - PowerPoint

Ashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste New Slide Section Slides

Clipboard markets, payment systems, and banks to steal money or block people from accessing the funds they need.

Font Paragraph

Text Direction Align Text Convert to SmartArt

Shapes Drawing Editing

Find Replace Select

35 Sunrise Attacks

These are the cyber equivalent of attacks like Pearl Harbor and 9/11. The point is to carry out a massive attack that the enemy isn't expecting, enabling the attacker to weaken their defenses

36 Cybercrime

Cybercrime is a crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Cybercrime may harm someone's security and financial health.

37 Cyber Crime Case Studies

On 21 May 2021, it was reported that Air India was subjected to a cyberattack whereas the personal details of about 4.5 million customers around the world were compromised including passport, credit card details, birth dates, name and ticket information.

38 Cyber Crime Case Studies

It was reported that the compromised servers by the hackers were later secured and Air India took steps by engaging external data security specialists. Air India also guaranteed its passengers that there was no conclusive evidence on whether any misuse of the personal data has been committed. The airlines also urged and encouraged the

# Sunrise Attacks

- These are the cyber equivalent of attacks like Pearl Harbor and 9/11.
- The point is to carry out a massive attack that the enemy isn't expecting, enabling the attacker to weaken their defenses

Unit 1 Nishant Doshi

Click to add notes

NOTES COMMENTS

Unit 1.pptx - PowerPoint

Aashka R -

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Slides

Clipboard

markets, payment systems, and banks to steal money or block people from accessing the funds they need.

35 Sunrise Attacks

- These are the cyber equivalent of attacks like Pearl Harbor and 9/11.
- The point is to carry out a massive attack that the enemy isn't expecting, enabling the attacker to weaken their defenses.

36 Cybercrime

- Cybercrime** is a crime that involves a computer and a network.
- The computer may have been used in the commission of a crime, or it may be the target. Cybercrime can harm someone's security and financial health.

37 Cyber Crime Case Studies

- On 24 May 2021, it was reported that Air India was subjected to a cyberattack whereas the personal details of about 4.5 million customers around the world were compromised including passport, credit card details, birth dates, name and ticket information.

38 Cyber Crime Case Studies

- It was reported that the compromised servers by the hackers were later seized and Air India took steps by engaging external data security specialists.
- Air India also assured its passengers that there is no conclusive evidence on whether any misuse of the personal data has been reported.
- The airlines also urged and encouraged the

Unit 1 Nishant Doshi

Click to add notes

NOTES COMMENTS

Unit 1.pptx - PowerPoint

Aashka R.

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste Clipboard Slides New Slide Section Reset Font Paragraph Drawing Editing

36 Cybercrime

- Cybercrime is a crime that involves a computer and a network.
- The computer may have been used in the commission of a crime, or it may be the target. Cybercrime may harm someone's security and financial health.

37 Cyber Crime Case Studies

- On 21 May 2021, it was reported that Air India was subjected to a cyberattack whereas the personal details of about 4.5 million customers around the world were compromised including passport, credit card details, birth dates, name and ticket information.

38 Cyber Crime Case Studies

- It was reported that the compromised servers by the hackers were later secured and Air India took steps by engaging external data security experts.
- Air India also guaranteed its passengers that there was no conclusive evidence on whether any misuse of the personal data has been reported.
- The airline also urged and encouraged the passengers to immediately change their passwords.

39 Cyber Crime Case Studies

- Vulnerabilities in the e-commerce domain of Indian bookseller **Oswaal Books** could have allowed attackers to seize control of the website, a security researcher has claimed.

40 Cyber Crime Case Studies

Click to add notes

Unit 1 Nishant Doshi

NOTES COMMENTS

The screenshot shows a Microsoft PowerPoint slide titled "Cyber Crime Case Studies". The slide has a blue header bar with the title. Below the title, there is a large text box containing a bulleted list of incidents. To the left of the slide, there are four small preview boxes labeled 36, 37, 38, and 39, each showing a snippet of the content from those slides. The bottom of the slide has a dark blue footer bar with the text "Unit 1 Nishant Doshi". The top of the image shows the PowerPoint ribbon and some navigation icons.

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Shape Fill Shape Outline Quick Styles Shape Effects

Find Replace Select

**Cybercrime**

- Cybercrime is a crime that involves a computer and a network.
- The computer may have been used in the commission of a crime, or it may be the target. Cybercrime may harm someone's security and financial health.

**Cyber Crime Case Studies**

37 Cyber Crime Case Studies

- On 24 May 2021, it was reported that Air India was subjected to a cyberattack whereas the personal details of about 4.5 million customers around the world were compromised including passport, credit card details, birth dates, name and ticket information.

38 Cyber Crime Case Studies

- It was reported that the compromised servers by the hackers were later secured and Air India took steps by engaging external data security specialists.
- Air India also guaranteed its passengers that there was no conclusive evidence on whether any misuse of the personal data has been reported.
- The airlines also urged and encouraged the passengers to immediately change their passwords.

39 Cyber Crime Case Studies

- Vulnerabilities in the e-commerce domain of Indian bookseller **Oswaal Books** could have allowed attackers to seize control of the website, a security researcher has claimed.

40 Cyber Crime Case Studies

Click to add notes

Unit 1 Nishant Doshi

NOTES COMMENTS

The screenshot shows a Microsoft PowerPoint slide titled "Cyber Crime Case Studies". The slide content includes a bulleted list of three case studies. The first case study is about Air India, mentioning a data breach in May 2021 where personal details of 4.5 million customers were compromised. Air India reportedly took steps to secure the servers and guaranteed no conclusive evidence of misuse. The second case study is about a vulnerability found in the e-commerce domain of Oswaal Books. The third case study is partially visible. The slide has a dark blue header and footer. The footer contains the text "Unit 1 Nishant Doshi". The slide number 40 is visible on the left side.

Unit 1.pptx - PowerPoint

Ashka R.

Cut Copy Format Painter New Slide Section

Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Shape Fill Shape Outline Shape Effects

Find Replace Select

LE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

**Cyber Crime Case Studies**

On 22 May 2021, it was reported that Air India was subjected to a cyberattack where the personal details of about 4.5 million customers around the world were compromised including passport, credit card details, birth dates, name and ticket information.

**Cyber Crime Case Studies**

- It was reported that the compromised services by the hackers were later secured and Air India took steps by engaging external data security specialists.
- Air India also guaranteed its passengers that there was no conclusive evidence on whether any misuse of the personal data has been reported.
- The airlines also urged and encouraged the passengers to immediately change their passwords.

**Cyber Crime Case Studies**

Vulnerabilities in the e-commerce domain of Indian bookseller **Oswaal Books** could have allowed attackers to seize control of the website, a security researcher has claimed.

**Cyber Crime Case Studies**

Vulnerabilities in the e-commerce domain of Indian bookseller **Oswaal Books** could have allowed attackers to seize control of the website, a security researcher has claimed.

**Cyber Crime Case Studies**

After taking control of the administrator account via SQL injection, the researcher achieved remote code execution (RCE), bypassed one-time password (OTP) authentication, and unearthed a cross-site request forgery (CSRF) bug, he claims.

**Cybercrimes Classification**

Click to add notes

Unit 1 Nishant Doshi

NOTES COMMENTS

Unit 1.pptx - PowerPoint

Ashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Effects

Find Replace Select

19 Cyber Crime Case Studies

- The airline also urged and encouraged the passengers to immediately change their passwords.

20 Cyber Crime Case Studies

- Vulnerabilities in the e-commerce domain of Indian book-seller **Oswaal Books** could have allowed attackers to seize control of the website, a security researcher has claimed.

40 Cyber Crime Case Studies

- After taking control of the administrator account via SQL injection, the researcher achieved remote code execution (RCE), bypassed one-time password (OTP) authentication, and unearthed a cross-site request forgery (CSRF) bug, he claims.

41 Cybercrimes Classification

- Against individual
  - Phishing:** Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as an individual or entity to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

42 Cybercrimes Classification (Contd.)

- Against individual
  - Sexting:** Sexting is the use of messaging systems to send multiple unsolicited messages to large numbers of people, usually for the purpose of harassment, for the purpose of non-commercial personal gain, or for the purpose of revealing sensitive information.
  - Password sniffing:** Password sniffing is an attack on the Internet that is used to steal user names and passwords from people. Most examples such as cracking and for sniffing password.

Cyber Crime Case Studies

- After taking control of the administrator account via SQL injection the researcher achieved remote code execution (RCE), bypassed one-time password (OTP) authentication, and unearthed a cross-site request forgery (CSRF) bug, he claims.

Unit 1 Nishant Doshi

Click to add notes

NOTES COMMENTS

39

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW Unit 1.pptx - PowerPoint Aashka R

Paste Cut Copy Format Painter New Slide Section Clipboard Slides

Vulnerabilities in the e-commerce domain of Indian bookseller Oswaal Books could have allowed attackers to seize control of the website, a security researcher has claimed.

40 Cyber Crime Case Studies

- After taking control of the administrator account via SQL injection the researcher achieved remote code execution (RCE), bypassed one-time password (OTP) authentication, and unearthed a cross-site request forgery (CSRF) bug, he claims.

41 Cybercrimes Classification

- Against Individual
  - EMAIL Spoofing: Email spoofing is a form of cyber attack in which a hacker sends an email that has been manipulated to seem as if it originated from a trusted source.
  - Phishing: Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

42 Cybercrimes Classification (Contd.)

- Against Individual
  - Spamming: Spamming is the use of messaging systems to send large volumes of unsolicited messages to large numbers of recipients for the purpose of commercial advertising, to spread political messages, or simply to annoy people by spamming or simply sending the same message over and over to the same user.
  - Password sniffing: Password sniffing is an attack on the network that intercepts and steals sensitive data, such as passwords, from the network. Man-in-the-middle attacks are commonly used for stealing passwords and credentials today.

43 Cybercrimes Classification (Contd.)

Click to add notes

Unit 1 Nishant Doshi

NOTES COMMENTS

The screenshot displays a Microsoft PowerPoint presentation titled 'Unit 1.pptx - PowerPoint'. The main slide, slide 41, is titled 'Cybercrimes Classification' and contains a bullet point list under the heading 'Against Individual'. The first item in this list is 'EMAIL Spoofing', described as a cyber attack where a hacker sends an email that appears to come from a trusted source. The second item is 'Phishing', defined as a cybercrime where targets are contacted by email, phone, or text to lure them into giving sensitive information like bank details or passwords. To the left of the main slide, there is a sidebar containing two other slides: 'Cyber Crime Case Studies' (slide 40) and 'Cybercrimes Classification (Contd.)' (slide 42). The 'Cyber Crime Case Studies' slide discusses a vulnerability in the e-commerce domain of Indian bookseller Oswaal Books. The 'Cybercrimes Classification (Contd.)' slide provides more details on 'Against Individual' attacks, specifically 'Spamming' and 'Password sniffing'. The bottom of the screen shows the standard PowerPoint navigation and ribbon tabs.

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste New Slide Reset Section Slides

Font Paragraph

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Effects

Shape Fill Shape Outline Shape Effects

Find Replace Select

Editing

# Cybercrimes Classification (Contd.)

• Against Individual

- Email Spamming: Email spamming is a form of cyber attack or other type of hacking where unsolicited messages are sent to multiple recipients as if it originated from a single source.
- Phishing: Phishing is a cybercrime in which a target or targets are contacted by email, telephone or even message by someone posing as a legitimate entity to trick victims into giving away sensitive information such as personally identifiable information, banking and credit card details, and passwords.

• Against Individual

- Spaming: Spaming is the use of messaging systems to send multiple unsolicited messages to large numbers of recipients for the purpose of commercial advertising, for the purpose of non-commercial proselytizing, for any prohibited purpose, or simply sending the same message over and over to the same user.
- Password sniffing: Password sniffing is an attack on the Internet that is used to steal user names and passwords from the network. Man-in-the-middle attacks are commonly used for stealing passwords and credentials today.

• Against property

- Credit card fraud: Credit card fraud is the unauthorized use of a credit or debit card, or similar payment tool (ACH, EFT, recurring charges, etc.), to fraudulently obtain money or property.

• Against property:

- Intellectual property:
- Patent infringement:
- Trade secret theft:
- Copyright infringement:

– Internet time theft: It refers to the theft in a manner where the unauthorized person uses internet hours paid by another person.

Unit 1 Nishant Doshi

Click to add notes

NOTES COMMENTS

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste New Slide Section Slides Font Paragraph Drawing Editing

Clipboard Layout Reset Text Direction Align Text Convert to SmartArt

Find Replace Select

42 Cybercrimes Classification (Contd.)

- Against individual:
  - Spoofing: Spoofing is the use of messaging systems to send phony (fake) messages to large numbers of people. It can be used for political advertising, by the sender of non-deliverable packages, or for spamming. It is also used for sending the same message over and over to the same user.
  - Password sniffing: Password sniffing is an attack on the network that intercepts the password and password from the network. Man-in-the-middle attacks are commonly used for stealing passwords and user credentials.

43 Cybercrimes Classification (Contd.)

- Against property:
  - Credit card fraud: Credit card fraud is the unauthorized use of a credit, debit card, or similar payment tool (ACH, EFT, recurring charge, etc.), to fraudulently obtain money or property.

44 Cybercrimes Classification (Contd.)

- Against property:
  - Intellectual property:
    - Patent infringement
    - Trademark infringement
    - Copyright infringement
  - Internet time theft: It refers to the theft in a manner where the unauthorized person uses internet hours paid by another person.

45 Cybercrimes Classification (Contd.)

- Against Organization:
  - Unauthorised accessing of computer
    - Virus Attacks
    - E-mail bombing
    - Trojan Horse
    - Software piracy

Unit 1 Nishant Doshi

Click to add notes

NOTES COMMENTS

85%

# Cybercrimes Classification (Contd.)

- Against property:
  - Credit card frauds: Credit card fraud is the unauthorized use of a credit or debit card, or similar payment tool (ACH, EFT, recurring charge, etc.), to fraudulently obtain money or property.

UNIT 1-PP01 - POWERPOINT

Aashka R -

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste New Slide Section Slides Font Paragraph Drawing Editing

Clipboard

Related entries: Phishing, Malware, Man-in-the-middle attack, Denial-of-service attack, Worm, Virus, Rootkit, Spyware, Trojan horse, Botnet, Ransomware,勒索软件, Phishing, Malware, Man-in-the-middle attack, Denial-of-service attack, Worm, Virus, Rootkit, Spyware, Trojan horse, Botnet, Ransomware

43 Cybercrimes Classification (Contd.)

- Against property:
  - Credit card fraud: Credit card fraud is an attack on the internet that is used to steal credit cards and personal information from victims. Malware and attacks are commonly used for stealing passwords and bank details today.

44 Cybercrimes Classification (Contd.)

- Against property:
  - Intellectual property:
    - Patent infringement:
    - Trademark infringement:
    - Copyright infringement:
  - Internet time theft: It refers to the theft in a manner where the unauthorized person uses internet hours paid by another person.

45 Cybercrimes Classification (Contd.)

- Against Organization:
  - Unauthorized access of computer
  - Virus Attacks
  - E-Mail Bomber
  - Trojan Horse
  - Software piracy

46 Cybercrimes Classification (Contd.)

- Against Society:
  - Forgery
  - Cyber Terrorism
  - Web Jacking

Click to add notes

Unit 1 Nishant Doshi

NOTES COMMENTS

43

44

45

46

# Cybercrimes Classification (Contd.)

- Against property:
  - Intellectual property:
    - Patent infringement:
    - Trademark infringement:
    - Copyright infringement:
  - Internet time theft: It refers to the theft in a manner where the unauthorized person uses internet hours paid by another person.
- Internet time theft: It refers to the theft in a manner where the unauthorized person uses internet hours paid by another person.

Unit 1.pptx - PowerPoint

Aashka R

Cut Copy Format Painter Paste New Slide Section Layout Reset Font Paragraph Drawing Editing

Clipboard Slides

44 Cybercrimes Classification (Contd.)

- Against property:
  - Credit card frauds, Credit card fraud is the unauthorized use of a credit or debit card, or similar payment card (ACH, EFT, recurring charges, etc.) to fraudulently obtain money or property.

45 Cybercrimes Classification (Contd.)

- Against Organization:
  - Unauthorized accessing of computer
    - Virus Attacks
    - E-Mail bombing
    - Trojan Horse
    - Software piracy

46 Cybercrimes Classification (Contd.)

- Against Society:
  - Forgery
  - Cyber Terrorism
  - Web Jacking

47 Indian ITA 2000

Click to add notes

Unit 1 Nishant Doshi

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cybercrimes Classification (Contd.)

15 Cybercrimes Classification (Contd.)

- Against Organization:
  - Unauthorized Accessing of Computer
  - Virus
  - Malware
  - Trojan Horse
  - Software piracy

16 Cybercrimes Classification (Contd.)

- Against Society:
  - Forgery
  - Cyber Terrorism
  - Web Jacking

47 Indian ITA 2000

48 Indian ITA 2000 (Contd.)

Click to add notes

Unit 1 Nishant Doshi

NOTES COMMENTS

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Clipboard Slides Font Paragraph Drawing Find Replace Select Editing

46 Cybercrimes Classification (Contd.)

- Against Society:
  - Forgery
  - Cyber Terrorism
  - Web Jacking

47 Indian ITA 2000

Table 1.7 | The key provisions under the Indian ITA 2000 (before the amendment)

Section Ref. and Title	Chapter of the Act and Title	Crime	Punishment
Sec. 43 (Penalty for damage to computer, computer system, etc.)	CHAPTER IX Penalties and Adjudication	Damage to computer system, etc.	Compensation for ₹ 1 crore (₹ 10,000,000).
Sec. 66 (Hacking with computer system)	CHAPTER XI Offences	Hacking (with intent or knowledge).	Fine of ₹ 2 lakhs (₹ 200,000) and imprisonment for 3 years.
Sec. 67 (Publishing of information which is obscene in electronic form)	CHAPTER XI Offences	Publication of obscene material in electronic form.	Fine of ₹ 1 lakh (₹ 100,000), imprisonment of 5 years and double conviction on second offence.

(Continued)

48 Indian ITA 2000 (Contd.)

49 CYBERTERRORISM

- Cyberterrorism is the premeditated, politically motivated attack against computers, computer systems, and data which result in violence against noncombatant targets sub national groups.
- Lack of information security gives rise to cybercrimes. Hence, the IT ACT 2000 and the TECNOLOGIES ACT 2008 provides new focus on Information security in India.

Click to add notes

47 Indian ITA 2000

48 Indian ITA 2000 (Contd.)

49 CYBERTERRORISM

- Cyberterrorism is the premeditated, politically motivated attack against information, computer systems. Computer programs and data which result in damage against noncombatant targets such as military groups.
- Lack of information security gives rise to cybercrimes. INDIAN INFORMATION TECHNOLOGY ACT ITA 2000 provides new focus on Information security in India.

50 Targets

- Targets may include power plants, military installation, the banking industry, air traffic control centers.

**Indian ITA 2000 (Contd.)**

**Table 1.7 | (Continued)**

Section Ref. and Title	Chapter of the Act and Title	Crime	Punishment
Sec. 68 (Power of controller to give directions)	CHAPTER XI Offences	Not complying with directions of controller.	Fine up to ₹ 2 lakhs (₹ 200,000) and imprisonment of 3 years.
Sec. 70 (Protected system)	CHAPTER XI Offences	Attempting or securing access to computer of another person without his/her knowledge.	Imprisonment up to 10 years.
Sec. 72 (Penalty for breach of confidentiality and privacy)	CHAPTER XI Offences	Attempting or securing access to computer for breaking confidentiality of the information of computer.	Fine up to ₹ 1 lakh (₹ 100,000) and imprisonment up to 2 years.
Sec. 73 (Penalty for publishing Digital Signature Certificate false in certain particulars)	CHAPTER XI Offences	Publishing false digital signatures, false in certain particulars.	Fine of ₹ 1 lakh (₹ 100,000) or imprisonment of 2 years or both.
Sec. 74 (Publication for fraudulent purpose)	CHAPTER XI Offences	Publication of Digital Signatures for fraudulent purpose.	Imprisonment for the term of 2 years and fine of ₹ 1 lakh (₹ 100,000).

Source: Information Technology Act 2000, Act no. 21, accessible at the URL: [http://www.commonlii.org/in/legis/num\\_act/ita2000258/](http://www.commonlii.org/in/legis/num_act/ita2000258/) (22 February 2000).

Click to add notes

Unit 1.pptx - PowerPoint

Aashika R.

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Layout Reset Font Paragraph Drawing Editing

Clipboard Slides

48 Indian ITA 2000 (Contd.)

49 CYBERTERRORISM

\* Cyberterrorism is the premeditated, politically motivated attack against information, computer systems, Computer programs and data which result in violence against noncombatant targets sub national groups.

Lack of information security gives rise to cybercrimes. INDIAN INFORMATION TECHNOLOGY ACT ITA 2000 provides new focus on Information security in india.

50 Targets

Targets may include power plants, military installation, the banking industry, air traffic control centers.

51 Targets (Contd.)

Click to add notes

Unit 1 Nishant Doshi

# CYBERTERRORISM

- **Cyberterrorism** is the premeditated, politically motivated attack against information, computer systems, Computer programs and data which result in violence against noncombatant targets sub national groups.
- Lack of information security gives rise to cybercrimes. INDIAN INFORMATION TECHNOLOGY ACT ITA 2000 provides new focus on Information security in india.

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste New Slide Section Reset Layout Section

Font Paragraph Drawing Editing

Targets

50 Targets

- Targets may include power plants, military installation, the banking industry, air traffic control centers.

51 Targets (Contd.)

```
graph TD; KeyTargets[Key targets] --> Military[Military]; KeyTargets --> Political[Political]; KeyTargets --> Economic[Economic]; KeyTargets --> Infrastructure[Infrastructure]
```

52 Cyber-Terrorism Challenges

- Difficulty Identifying Attackers: It remains difficult to determine the identity of the initiators of most cyber attacks.
- Lack of boundaries: Attacks can originate from anywhere in the world and from multiple locations.
- Speed of development: The time between discovery of a new vulnerability and the emergence of a new tool or technique that exploits the vulnerability is getting shorter.

53 Cyber Terrorism Challenges

- Low cost tools: The technology employed in attacks is simple to use, inexpensive, and

Click to add notes

Unit 1 Nishant Doshi

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy New Slide Section Layout Reset Text Direction Align Text Convert to SmartArt

Font Paragraph Drawing Find Replace Select Editing

Targets may include power plants, military installation, the banking industry, air traffic control centers.

Targets (Contd.)

Targets (Contd.)

51 Cyber Terrorism Challenges

- Difficulty identifying attackers; it remains difficult to determine the identity of the initiators of most cyber attacks.
- Lack of boundaries: Attacks can originate from anywhere in the world and from multiple locations.
- Speed of operation: The time between the discovery of a new vulnerability and the emergence of a new tool or technique that exploits the vulnerability is getting shorter.

52 Cyber-Terrorism Challenges

- Low-cost tools: The technology employed in attacks is simple to use, inexpensive, and widely available.
- Automated Methods: The methods of attack have become automated and more sophisticated, resulting in greater damage from a single attack.

53 Cyber Terrorism Forms

- Privacy violation.
- Secret information appropriation and data

54 Targets (Contd.)

## Targets (Contd.)

```
graph TD; A[Cyber Terrorism Targets] --> B[Private industry or entities]; A --> C[Government cyber and physical infrastructure]; A --> D[Social and national identity]; A --> E[Critical national infrastructures]; A --> F[Military and forces cyber and physical infrastructure]
```

Click to add notes

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Shapes Shape Fill Shape Outline Quick Styles Shape Effects Select

Targets may include power plants, military installation, the banking industry, air traffic control centers.

51 Targets (Contd.)

```
graph TD; Targets[Targets] --> Infrastructure[Infrastructure]; Targets --> Financial[Financial]; Targets --> Military[Military]; Targets --> Transportation[Transportation]; Targets --> Civilian[Civilian]
```

52 Cyber Terrorism Challenges

- Difficulty Identifying Attackers: It remains difficult to determine the identity of the initiators of most cyber attacks.
- Lack of boundaries: Attacks can originate from anywhere in the world and from multiple locations simultaneously.
- Speed of development: The time between the discovery of a new vulnerability and the emergence of a new tool or technique that exploits the vulnerability is getting shorter.

53 Cyber Terrorism Challenges

- Low cost tools: The technology employed in attacks is simple to use, inexpensive, and widely available.
- Automated Methods: The methods of attack have become automated and more sophisticated, resulting in greater damage from a single attack.

54 Cyber Terrorism Forms

- Privacy violation.
- Secret information appropriation and data

Unit 1 Nishant Doshi

Click to add notes

NOTES COMMENTS

Unit 1.pptx - PowerPoint

Aashka R

Cyber Terrorism Challenges

- Difficulty identifying terrorists; it remains difficult to determine the identity of the initiators of most cyber attacks.
- Low cost tools: Terrorists can organize fraud anywhere in the world and from multiple locations simultaneously.
- Speed of execution: The time between the discovery of a new vulnerability and the emergence of a new tool or technique that exploits the vulnerability is getting shorter.

Cyber Terrorism Challenges

- Low cost tools: The technology employed in attacks is simple to use, inexpensive, and widely available.
- Automated Methods: The methods of attack have become automated and more sophisticated, resulting in greater damage from a single attack.

Cyber Terrorism Forms

- Privacy violation.
- Secret information appropriation and data theft.
- Demolition of e-governance base.
- Distributed Denial Of Service (DoS) attack.
- Network damage and disruptions.
- Use of cyber communication for terrorism.

Attack Methods

- Physical Attack:**
  - Against computer facilities and/or transmission lines.
  - Against personnel of organizational networks to destroy or severely injure computer and their terminals.
- Electrical Attacks:**
  - Use of power of electromagnetic energy or electromagnetic pulse to overwhelm computer circuitry.
- Other Attacks:**
  - Use of malicious code to take advantage of software's weakness.

Click to add notes

Unit 1 Nishant Doshi

NOTES COMMENTS

Unit 1.pptx - PowerPoint

Aashka R

Cut Copy Format Painter New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Fill Shape Outline Shape Effects Select

**Cyber Terrorism Challenges**

- Low cost tools: The technology employed in attacks is simple to use, inexpensive, and widely available.
- Automated Methods: The methods of attack have become automated and more sophisticated, resulting in greater damage from a single attack.

**Cyber Terrorism Forms**

- Privacy violation.
- Secret information appropriation and data theft.
- Demolition of e-governance base.
- Distributed Denial Of Service (DoS) attack.
- Network damage and disruptions.
- Use of cyber communication for terrorism.

**Attack Methods**

- Physical Attack:
  - Attack similar to that of conventional wars.
  - Attacked by use of conventional weapons to destroy or seriously injure computer and their owners.
- Electronic Attack:
  - Use of power of electromagnetic energy or other electronic pulses to overload computer circuitry.
  - Cyber Attack:
    - Use of malicious code to take advantage of software's weakness.

**Cyber Terrorism Tools**

- Virus:
- Worms:
- Trojan Horse:
- Logic Bombs:
- Trap Doors:
- DoS:
- Cryptography:
- Steganography:

Click to add notes

Unit 1 Nishant Doshi

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Slides

Clipboard

exploits the vulnerability is getting shorter.

53 Cyber Terrorism Challenges

- Low cost tools: The technology employed in attacks is simple to use, inexpensive, and widely available.
- Automated Methods: The methods of attack have become automated and more sophisticated, resulting in greater damage from a single attack.

54 Cyber Terrorism Forms

- Privacy violation.
- Secret information appropriation and data theft.
- Derivation of e-governance base.
- Distributed Denial Of Service (DoS) attack.
- Network damage and disruptions.
- Use of cyber communication for terrorism.

55 Attack Methods

- Physical Attack:
  - Against computer facilities and/or transmission lines.
  - Accomplished by use of conventional weapons to destroy or seriously injure computer and their terminal.
- Electronic Attack:
  - Use of power of electromagnetic energy or electromagnetic pulse to overload computer circuitry.
- Cyber Attack:
  - Use of malicious code to take advantage of software's weakness.

56 Cyber Terrorism Tools

- Virus:
- Worms:
- Trojan Horse:
- Logic Bombs:
- Trap Doors:
- DoS:
- Cryptography:
- Steganography:

Click to add notes

Unit 1 Nishant Doshi

Annotations: COMMENTS

The screenshot shows a Microsoft PowerPoint slide titled "Attack Methods". The slide is divided into three main sections: "Physical Attack", "Electronic Attack", and "Cyber Attack". Each section has a list of sub-points. The slide is part of a presentation titled "Unit 1.pptx". The left side of the screen shows a navigation pane with slide thumbnails labeled 53, 54, 55, and 56. The top of the screen shows the PowerPoint ribbon with tabs like FILE, HOME, INSERT, DESIGN, etc. The right side of the screen shows the "Drawing" tab of the ribbon.

The screenshot shows a Microsoft PowerPoint slide titled "Cyber Terrorism Tools". The slide contains a bulleted list of nine tools. In the bottom-left corner of the slide area, there is a red rectangular box highlighting the first item in the list: "Virus:". The status bar at the bottom of the slide indicates "Unit 1 Nishant Doshi". The left sidebar of the PowerPoint interface displays a navigation pane with sections like "Cyber Terrorism Forms", "Attack Methods", and a summary section titled "Cyber Terrorism Tools" which lists the same nine items as the slide.

Unit 1.pptx - PowerPoint

HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section

Layout Reset Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Shape Fill Shape Outline Quick Styles Shape Effects

Find Replace Select

**Cyber Terrorism Tools**

- Virus:
- Worms:
- Trojan Horse:
- Logic Bombs:
- Trap Doors:
- DoS:
- Cryptography:
- Steganography:

6

57

THE 7 LAYERS OF CYBERSECURITY

Click to add notes

Unit 1.pptx - PowerPoint

Aashka R.

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Slides

Clipboard

Physical Attack: Accomplished by use of conventional weapons to destroy or severely injure computer and their systems.

Electronic Attack: Use of power of electromagnetic energy or microwave pulse to overload computer memory.

Cyber Attack: Use of malicious code to take advantage of software and hardware.

Font Paragraph Drawing Editing

Find Replace Select

Click to add title

## THE 7 LAYERS OF CYBERSECURITY

THE HUMAN LAYER

PERIMETER SECURITY

NETWORK SECURITY

ENDPOINT SECURITY

APPLICATION SECURITY

DATA SECURITY

MISSION CRITICAL ASSETS

Unit 1 Nishant Doshi

56

Cyber Terrorism Tools

- Virus:
- Worms:
- Trojan Horse:
- Logic Bombs:
- Trap Doors:
- Dos:
- Cryptography:
- Steganography:

57

THE 7 LAYERS OF CYBERSECURITY

58

- 1: Mission Critical Assets – This is the data you need to protect.
- 2: Data Security – Data security controls protect the storage and transfer of data.
- 3: Application Security – Application security controls access to an application, an application's access to your mission critical assets, and the internal security of the application.
- 4: Endpoint Security – Endpoint security controls protect the connection between devices and the network.

59

- 5: Network Security – Network security controls protect an organization's network and prevent unauthorized access of the network.
- 6: Perimeter Security – Perimeter security

Click to add notes

57

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Shape Fill Shape Outline Quick Styles Shape Effects Select

Find Replace

Aashka R

58

• 1: Mission Critical Assets – This is the data you need to protect.

• 2: Data Security – Data security controls protect the storage and transfer of data.

• 3: Application Security – Applications security controls protect access to an application; an application's access to your mission critical assets, and the internal security of the application.

• 4: Endpoint Security – Endpoint security controls protect the connection between devices and the network.

59

• 5: Network Security – Network security controls protect an organization's network and prevent unauthorized access.

• 6: Perimeter Security – Perimeter security controls include both the physical and digital security methodologies that protect the business overall.

60

• 7: The Human Layer – Humans are the weakest link in any cyber security posture. Human security controls include phishing simulations and access management controls that protect mission critical assets from a wide variety of human threats, including cyber criminals, malicious insiders, and negligent users.

61

Click to add title

- 1: Mission Critical Assets – This is the data you need to protect
- 2: Data Security – Data security controls protect the storage and transfer of data.
- 3: Application Security – Applications security controls protect access to an application, an application's access to your mission critical assets, and the internal security of the application.
- 4: Endpoint Security – Endpoint security controls protect the connection between devices and the network.

Click to add notes

Unit 1 Nishant Doshi

58

```
graph TD; Admin[Central Admin] --> Sales[Sales]; Admin --> Marketing[Marketing]; Admin --> HR[HR]; Sales --> SalesTeam[Sales Team]; SalesTeam --> SalesRep1[Sales Rep 1]; SalesTeam --> SalesRep2[Sales Rep 2]; SalesTeam --> SalesRep3[Sales Rep 3]
```



FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Shape Fill Shape Outline Quick Styles Shape Effects

Find Replace Select

Aashka R

59

• 5: Network Security – Network security controls protect an organization's network and prevent unauthorized access of the network.

• 6: Perimeter Security – Perimeter security controls include both the physical and digital security methodologies that protect the business overall.

60

• 7: The Human Layer – Humans are the weakest link in any cyber security posture. Human security controls include phishing simulations and access management controls that protect mission critical assets from a wide variety of human threats, including cyber criminals, malicious insiders, and negligent users.

[No Title]

61

• Cyber Human Actions

```
graph TD; A[Cyber Human Actions] --> B[Insider]; A --> C[Outsider]; A --> D[Malicious]; B --> E[Phish]; B --> F[Exploit]; B --> G[Leave Colab]
```

62

• inadvertent actions (generally by insiders) that are taken without malicious or harmful intent;

Click to add title

● 7: The Human Layer – Humans are the weakest link in any cyber security posture. Human security controls include phishing simulations and access management controls that protect mission critical assets from a wide variety of human threats, including cyber criminals, malicious insiders, and negligent users.

Click to add notes

Unit 1 Nishant Doshi 60

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy New Slide Section Reset Format Painter Clipboard

1 \* 12 \* 53 \* 64 \*

Click to add title

- inadvertent actions (generally by insiders) that are taken without malicious or harmful intent;

1 inadvertent actions (generally by insiders) that are taken without malicious or harmful intent;

2 deliberate actions (by insiders or outsiders) that are taken intentionally and are meant to do harm;

3 intention (generally by insiders), such as a failure to act in a given situation, either because of a lack of appropriate skills, knowledge, guidance, or availability of the correct person to take action Of primary concern

Unit 1 Nishant Doshi

62

NOTES COMMENTS

Click to add notes

Unit 1.pptx - PowerPoint

Aashka R

**FILE** **HOME** **INSERT** **DESIGN** **TRANSITIONS** **ANIMATIONS** **SLIDE SHOW** **REVIEW** **VIEW**

Cut Copy Format Painter Paste New Slide Section Reset Layout

Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Fill Shape Outline Shape Effects Select

**Click to add title**

• deliberate actions (by insiders or outsiders) that are taken intentionally and are meant to do harm;

12 • inadvertent actions (generally by insiders) that are taken without malicious or harmful intent;

53 • deliberate actions (by insiders or outsiders) that are taken intentionally and are meant to do harm;

64 • inaction (generally by insiders), such as a failure to act in a given situation, either because of a lack of appropriate skills, knowledge, guidance, or availability of the correct person to take action. Of primary concern

[No Title]

65 • Political motivations: examples include destroying, disrupting, or taking control of targets; espionage; and making political statements, protests, or retaliatory actions.

Click to add notes

Unit 1 Nishant Doshi 63

This screenshot shows a Microsoft PowerPoint slide titled 'Click to add title'. The slide contains a single bullet point: '• deliberate actions (by insiders or outsiders) that are taken intentionally and are meant to do harm;'. On the left side of the screen, there is a vertical list of slide thumbnails, numbered 12, 53, 64, and 65. Each thumbnail contains a small portion of the slide content. At the bottom of the slide, there is a footer bar with the text 'Unit 1 Nishant Doshi' and the number '63'.

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste New Slide Section Layout Reset

Clipboard Slides

Font Paragraph

Drawing Editing

Find Replace Select

52 • inadvertent actions (generally by insiders) that are taken without malicious or harmful intent.

63 • deliberate actions (by insiders or outsiders) that are taken intentionally and are meant to do harm.

64 • inaction (generally by insiders), such as a failure to act in a given situation, either because of a lack of appropriate skills, knowledge, guidance, or availability of the correct person to take action Of primary concern

65 • Political motivations: examples include destroying, disrupting, or taking control of targets; espionage; and making political statements, protests, or retaliatory actions.

Click to add title

- inaction (generally by insiders), such as a failure to act in a given situation, either because of a lack of appropriate skills, knowledge, guidance, or availability of the correct person to take action Of primary concern

Click to add notes

Unit 1 Nishant Doshi 64

The screenshot shows a Microsoft PowerPoint slide titled "Click to add title". The main content area contains a single bullet point: "• inaction (generally by insiders), such as a failure to act in a given situation, either because of a lack of appropriate skills, knowledge, guidance, or availability of the correct person to take action Of primary concern". On the left side of the slide, there are four numbered callouts (52, 63, 64, 65) pointing to specific text blocks on the previous slide. The top navigation bar includes FILE, HOME, INSERT, DESIGN, TRANSITIONS, ANIMATIONS, SLIDE SHOW, REVIEW, and VIEW tabs. The ribbon also shows sections for CLIPBOARD, LAYOUT, and DRAWING. The status bar at the bottom right indicates the slide number (64) and the author's name (Nishant Doshi).

Unit 1.pptx - PowerPoint

Aashka R -

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Shape Fill Shape Outline Quick Styles Shape Effects

Find Replace Select

64

65

66

67

Click to add title

- **Political motivations:** examples include destroying, disrupting, or taking control of targets; espionage; and making political statements, protests, or retaliatory actions.

Click to add notes

Unit 1 Nishant Doshi 65

NOTES COMMENTS

Unit 1.pptx - PowerPoint

Aashka R

Cut Copy Format Painter New Slide Reset Section Clipboard Slides Font Paragraph Drawing Editing

Clipboard Slides Font Paragraph Drawing Editing

66

• Economic motivations: examples include theft of intellectual property or other economically valuable assets (e.g., funds, credit card information); fraud; industrial espionage and sabotage; and blackmail.

67

• Socio-cultural motivations: examples include attacks with philosophical, ideological, political, and even religious intent. Socio-cultural motivations also include fun, curiosity, and a desire for publicity or ego gratification.

68

Attacks

69

• Injection attacks

• It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information.

Click to add title

• **Economic motivations:** examples include theft of intellectual property or other economically valuable assets (e.g., funds, credit card information); fraud; industrial espionage and sabotage; and blackmail.

• **Socio-cultural motivations:** examples include attacks with philosophical, ideological, political, and even religious intent. Socio-cultural motivations also include fun, curiosity, and a desire for publicity or ego gratification.

Unit 1 Nishant Doshi

66

Click to add notes

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Paste Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Outline Shape Effects Select

Find Replace

Click to add title

- **Socio-cultural motivations:** examples include attacks with philosophical, theological, political, and even humanitarian goals. Socio-cultural motivations also include fun, curiosity, and a desire for publicity or ego gratification.

58 Attacks

- Injection attacks
  - It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information.
  - Example- SQL Injection, code Injection, log Injection, XML Injection etc.

69

- DNS Spoofing
  - DNS Spoofing is a type of computer security hacking. Whereby a data is introduced into a DNS resolver's cache with a fake name and IP address, returning the correct IP address, diverting traffic to the attacker computer or any other computers. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.

70 Click to add notes

71

Unit 1 Nishant Doshi 67

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Paste Format Painter New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Effects

Find Replace Select

7

- Socio-cultural motivations: examples include attacks with philosophical, theological, political, and even humanitarian goals. Socio-cultural motivations also include fun, curiosity, and a desire for publicity or ego gratification.

8

Attacks

59

- Injection attacks
- It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information.
- Example- SQL injection, code injection, log injection, XML Injection etc.

70

- DNS Spoofing
- DNS Spoofing is a type of computer security hacking. Whereby a data is introduced into a DNS resolver's cache changing the name server's records and causing the attack to divert traffic to the attacker's computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.

68

Click to add notes

Attacks

Click to add subtitle

Click to add notes

The screenshot shows a Microsoft Word document with a slide titled "Click to add title". The slide contains the following bullet points:

- **Injection attacks**
- 
- It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information.
- 
- **Example-** SQL Injection, code Injection, log Injection, XML Injection etc.

The Word ribbon is visible at the top, showing tabs like FILE, HOME, DESIGN, TRANSITIONS, ANIMATIONS, SLIDE SHOW, REVIEW, and VIEW. The left margin of the slide has a list of notes from the previous slide:

- 67 • Socio-cultural motivations: examples include attacks with philosophical, theological, political, and even humanitarian goals. Socio-cultural motivations also include fun, curiosity, and a desire for publicity or ego gratification.
- 68 Attacks
- 69 • Injection attacks.
  - It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information.
  - 
  - Example- SQL Injection, code Injection, log Injection, XML Injection etc.
- 70 • DNS Spoofing
  - DNS Spoofing is a type of computer security hazard that occurs when a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attacker's computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.
- 71 Click to add notes

At the bottom of the slide, it says "Unit 1 Nishant Doshi" and the page number "69".

Unit 1.pptx - PowerPoint

Aashka R.

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Effects Select

Clipboard Slides

Click to add title

59

- Injection attacks
- It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information.
- Example- SQL Injection, code injection, log injection, XML Injection etc.

70

- DNS Spoofing
- DNS Spoofing is a type of computer security hacking. Whereby a data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attackers computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.

71

- Session Hijacking
- It is a security attack on user sessions over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.

72

- Phishing
- Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.

Unit 1 Nishant Doshi

Click to add notes

70

NOTES COMMENTS

Unit 1.pptx - PowerPoint

Aashka R.

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy New Slide Section Format Painter Slides

Clipboard application and fetch the required information.

Example: SQL Injection, code Injection, log Injection, XML Injection etc.

Font

Paragraph

Drawing

Editing

Find Replace Select

70

★

- DNS Spoofing
- DNS Spoofing is a type of computer security hacking. Whereby a data is introduced into a DNS resolver's cache resulting the name server to resolve the IP address of the website specific to the attacker's computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.

71

★

- Session Hijacking
- It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.

[No Title]

72

★

- Phishing
- Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.

73

★

- Brute force
- It is a type of attack which uses a trial and error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to

Click to add title

● **Session Hijacking**

- 
- **It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.**

Click to add notes

Unit 1 Nishant Doshi

71

NOTES COMMENTS

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Slides

Font Paragraph Drawing Editing

Session Hijacking

- It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.

Phishing

- Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.

Brute force

- It is a type of attack which uses a trial-and-error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security analysts to test an organization's network security.

Denial of Service

- It is an attack which recurs to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash. It uses the single system and single internet connection to attack a server.

Click to add title

- Phishing**
- 
- Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.

Click to add notes

Unit 1 Nishant Doshi

72

73

74

75

SIDE 72 OF 96 ENGLISH (INDIA)

Type here to search

13:38 09-02-2024

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Find Replace Select

71 Session Hijacking

- It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.

72 Phishing

- Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.

73 Brute force

- It is a type of attack which uses a trial and error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security analysts to test an organization's network security.

74 Denial of Service

- It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash, like the single system and single internet connection to attack a server.

75 Click to add notes

Click to add title

● Brute force

- 
- It is a type of attack which uses a trial and error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security analysts to test an organization's network security.

Unit 1 Nishant Doshi

73

NOTES COMMENTS

Unit 1.pptx - PowerPoint

Aashka R -

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Find Replace Select

73

★

- Brute force
  - It is a type of attack which uses a trial and error method. This attack generates a large number of possible combinations of user credentials like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security analysts to test an organization's network security.

74

★

- Denial of Service
  - It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash. It uses the single system and single internet connection to attack a server.

75

★

- Dictionary attacks
  - This type of attack stored the list of a commonly used password and validated them to get original password.

76

★

- URL Interpretation
  - It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.

77

Click to add title

• Denial of Service

- 
- It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash. It uses the single system and single internet connection to attack a server.

Unit 1 Nishant Doshi

74

Click to add notes

NOTES COMMENTS

Unit 1.pptx - PowerPoint

Aashka R

HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Fill Shape Outline Find Replace Select

Brute force

- It is a type of attack which uses a trial and error method. This attack generates a large number of questions and validates them against the data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security analysts to test an organization's network security.

Denial of Service

- It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash. It uses the single system and single internet connection to attack a server.

Dictionary attacks

- This type of attack stored the list of a commonly used password and validated them to get original password.

URL Interpretation

- It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.

Click to add title

Click to add notes

Unit 1 Nishant Doshi

75

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Effects

Find Replace Select

75

★

- Dictionary attacks
- This type of attack stored the list of a commonly used password and validated them to get original password.

76

★

- URL Interpretation
- It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.

77

★

- File Inclusion attacks
- It is a type of attack that allows an attacker to access unauthorized or essential files which is available on the web server or to execute malicious files on the web server by making use of the include functionality.

78

★

- Man in the middle attacks
- It is a type of attack that allows an attacker to intercepts the connection between client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.

Click to add title

● URL Interpretation

- 
- It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.

Click to add notes

Unit 1 Nishant Doshi

76

NOTES COMMENTS

Unit 1.pptx - PowerPoint

Aashka R -

LE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy New Slide Reset Section Format Painter

Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Effects Select

Click to add title

**• File Inclusion attacks**

- It is a type of attack that allows an attacker to access unauthorized or essential files which is available on the web server or to execute malicious files on the web server by making use of the include functionality.

5

6

7

8

77

78

• File Inclusion attacks

- It is a type of attack that allows an attacker to access unauthorized or essential files which is available on the web server or to execute malicious files on the web server by making use of the include functionality.

Click to add notes

Unit 1 Nishant Doshi

77

Unit 1.pptx - PowerPoint

Aashka R.

HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Reset Section

Clipboard Slides

JRI Interpretation

It is a type of attack where we can change the certain parts of a URL and one can make a web server to deliver web pages for which he is not authorized to browse.

File Inclusion attacks

It is a type of attack that allows an attacker to access unauthorized or essential files which is available on the web server or to execute malicious files on the web server by making use of the include functionality.

Man in the middle attacks

It is a type of attack that allows an attacker to intercept the connection between client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.

Virus

It is a type of malicious software program that spreads throughout the computer files without the user's knowledge. It is a type of malicious computer program that replicates by inserting copies of itself into other computer programs when executed. It can also execute instructions that cause harm to the system.

Click to add title

● Man in the middle attacks

- 
- It is a type of attack that allows an attacker to intercepts the connection between client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.

Click to add notes

Unit 1 Nishant Doshi

78

The screenshot shows a Microsoft Word document with a slide titled "Click to add title". The slide contains the following bullet points:

- Virus
- It is a type of malicious software program that spread throughout the computer files without the knowledge of a user. It is a self-replicating malicious computer program that replicates by inserting copies of itself into other computer programs when executed. It can also execute instructions that cause harm to the system.

On the left side of the screen, there is a vertical list of slide thumbnails numbered 78, 79, 80, and 81. Each thumbnail has a small preview of its content. The thumbnails for slides 78, 79, and 80 are highlighted with a red border. The thumbnails for slides 78 and 79 contain text about "Man in the middle attacks" and "Virus" respectively. The thumbnail for slide 80 contains text about "Worm". The thumbnail for slide 81 contains text about "Trojan horse".

At the bottom of the slide, there is a footer bar with the text "Unit 1 Nishant Doshi" and the number "79" on the right side.

The screenshot shows a Microsoft Word document with a presentation slide open. The slide has a blue header bar with the placeholder "Click to add title". The main content area contains a bulleted list:

- Worm
- It is a type of malware whose primary function is to replicate itself to spread to uninfected computers. It works same as the computer virus. Worms often originate from email attachments that appear to be from trusted senders.

Below the slide, there is a note section with the placeholder "Click to add notes". The Word ribbon is visible at the top, showing tabs like FILE, HOME, INSERT, DESIGN, TRANSITIONS, ANIMATIONS, SLIDE SHOW, REVIEW, and VIEW. The left sidebar lists other slides in the presentation, numbered 79, 80, 81, and 82, each with a preview of its content.

UNIT 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Layout Reset

Clipboard Slides Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Effects

Find Replace Select

UNIT 1.pptx - PowerPoint

80 ★

- Worm
  - It is a type of malware whose primary function is to replicate itself to spread to uninfected computers. It works same as the computer virus. Worms often originate from email attachments that appear to be from trusted senders.

81 ★

- Trojan horse
  - It is a malicious program that occurs unexpected changes to computer setting and unusual activity, even when the computer should be idle. It misleads the user of its true intent. It appears to be a normal application but when opened/executed some malicious code will run in the background.

82 ★

- Backdoors
  - It is a method that bypasses the normal authentication process. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.

83 ★

- Bots
  - A bot (short for "robot") is an automated process that interacts with other network services. Some bots program run automatically, while others only execute commands when they receive specific input. Common examples of bots program are the crawler, chatroom bots, and malicious bots.

Click to add title

- **Trojan horse**
- 
- **It is a malicious program that occurs unexpected changes to computer setting and unusual activity, even when the computer should be idle. It misleads the user of its true intent. It appears to be a normal application but when opened/executed some malicious code will run in the background.**

Click to add notes

Unit 1 Nishant Doshi

81

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Effects

Find Replace Select

80

★ • Worm  
• It is a type of malware whose primary function is to replicate itself to spread to uninfected computers. It works same as the computer virus. Worms often originate from email attachments that appear to be from trusted senders.

81

★ • Trojan horse  
• It is a malicious program that occurs unexpected changes to computer setting and unusual activity, even when the computer should be idle. It misleads the user of its true intent. It appears to be a normal application but when opened/executed some malicious code will run in the background.

82

★ • Backdoors  
• It is a method that bypasses the normal authentication process. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.

83

★ • Bots  
• A bot (short for "robot") is an automated process that interacts with other network services. Some bots program run automatically, while others only execute commands when they receive specific input. Common examples of bots program are the crawler, chatroom bots, and malicious bots.

84

★ • Session replay In this type of attack, a hacker

Click to add title

● **Backdoors**

●

● **It is a method that bypasses the normal authentication process. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.**

Unit 1 Nishant Doshi

82

Click to add notes

NOTES COMMENTS

Unit 1.pptx - PowerPoint

Aashka R

Cut Copy Format Painter Layout New Slide Section Paste Clipboard Slides Font Paragraph Drawing Editing

82

• Backdoors

- It is a method that bypasses the normal authentication process. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.

83

• Bots

- A bot (short for "robot") is an automated process that interacts with other network services. Some bots program run automatically, while others only execute commands when they receive specific input. Common examples of bots program are the crawler, chatroom bots, and malicious bots.

84

• Session replay: In this type of attack, a hacker steals an authorized user's log in information by stealing the session ID. The intruder gains access and the ability to do anything the authorized user can do on the website.

85

• Message modification: In this attack, an intruder alters packet header addresses to direct a message to a different destination or modify the data on a target machine.

86

Click to add title

- **Bots**
- A bot (short for "robot") is an automated process that interacts with other network services. Some bots program run automatically, while others only execute commands when they receive specific input. Common examples of bots program are the crawler, chatroom bots, and malicious bots.

Click to add notes

Unit 1 Nishant Doshi

83

Unit 1.pptx - PowerPoint

Aashka R -

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Fill Shape Outline Shape Effects

Find Replace Select

Click to add title

- **Session replay:** In this type of attack, a hacker steals an authorized user's log in information by stealing the session ID. The intruder gains access and the ability to do anything the authorized user can do on the website.

84

85

86

Unit 1 Nishant Doshi 84

Click to add notes

The screenshot shows a Microsoft PowerPoint slide titled "Click to add title". The slide content is as follows:

- **Session replay:** In this type of attack, a hacker steals an authorized user's log in information by stealing the session ID. The intruder gains access and the ability to do anything the authorized user can do on the website.

The slide is numbered 84 at the bottom right. On the left, there are thumbnails of other slides, some of which contain text about network attacks like "Blackdoors" and "Bots". The top ribbon shows standard PowerPoint tabs: FILE, HOME, INSERT, DESIGN, TRANSITIONS, ANIMATIONS, SLIDE SHOW, REVIEW, and VIEW. The ribbon also includes various font and paragraph styles, drawing tools, and search functions.

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Shape Fill Shape Outline Quick Styles Shape Effects

Find Replace Select

84

85

86

87

Click to add title

- **Message modification:** In this attack, an intruder alters packet header addresses to direct a message to a different destination or modify the data on a target machine.

Unit 1 Nishant Doshi

85

Click to add notes

SLIDE 85 OF 96 ENGLISH (INDIA)

Type here to search

13:38 09.02.2024

Unit 1.pptx - PowerPoint

Aashka R

HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Layout Reset

Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Effects

Find Replace Select

Session replay: In this type of attack, a hacker steals an authorized user's log in information by stealing the session ID. The intruder gains access and the ability to do anything the authorized user can do on the website.

Message modification: In this attack, an intruder alters packet header addresses to direct a message to a different destination or modify the data on a target machine.

In a distributed denial-of-service (DDoS) exploit, large numbers of compromised systems (sometimes called a botnet or zombie army) attack a single target.

• In a distributed denial-of-service (DDoS) exploit, large numbers of compromised systems (sometimes called a botnet or zombie army) attack a single target.

7 • Confidentiality (manipulation): the attacker simply steals the messages exchanged by two entities. For the attack to be useful, the traffic must not be encrypted. Any unencrypted information, such as a password sent in response to an HTTP request, may be retrieved by the attacker.

88 • Traffic analysis: the attacker looks at the metadata transmitted in traffic in order to deduce

Click to add title

Click to add notes

Unit 1 Nishant Doshi 86

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Effects

Find Replace Select

Click to add title

86

- In a **distributed denial-of-service (DDoS)** exploit, large numbers of compromised systems (sometimes called a botnet or zombie army) attack a single target.

87

- Eavesdropping (tapping):** the attacker simply listens to messages exchanged by two entities. For the attack to be useful, the traffic must not be encrypted. Any unencrypted information, such as a password sent in response to an HTTP request, may be retrieved by the attacker.

88

- Traffic analysis:** the attacker looks at the metadata transmitted in traffic in order to deduce information relating to the exchange and the participating entities, e.g. the form of the exchanged traffic (rate, duration, etc.). In the case of encrypted traffic, traffic analysis can also lead to attacks by **cryptanalysis**, whereby the attacker may obtain information or succeed in unencrypting the traffic.

89

- Software Attacks:** Malicious code (sometimes called **malware**) is a type of software designed to take over or damage a computer user's operating system, without the user's knowledge or approval. It can be very difficult to remove and very damaging.

Click to add notes

Unit 1 Nishant Doshi 87

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Clipboard Slides Font Paragraph Drawing Editing

87

- **Session hijacking**: the attacker simply listens to messages exchanged by two entities. For the session to succeed, the traffic must not be encrypted. Any unencrypted information, such as a password sent in response to an HTTP request, may be retrieved by the attacker.

88

- **Traffic analysis**: the attacker looks at the metadata transmitted in traffic in order to deduce information relating to the exchange and the participating entities, e.g. the form of the exchanged traffic (rate, duration, etc.). In the cases where encrypted data are used, traffic analysis can also lead to attacks by cryptanalysis, whereby the attacker may obtain information or succeed in unencrypting the traffic.

89

- **Software Attacks**: Malicious code (sometimes called malware) is a type of software designed to take over and damage a computer user's operating system, without the user's knowledge or approval. It can be very difficult to remove and very damaging.

90

- **Need of Security policies**
  - 1. It increases efficiency.
  - 2. It provides interoperability.
  - 3. It can reduce or break a system that.
  - 4. Helps in reducing compliance on security.

Click to add title

● **Traffic analysis:** the attacker looks at the metadata transmitted in traffic in order to deduce information relating to the exchange and the participating entities, e.g. the form of the exchanged traffic (rate, duration, etc.). In the cases where encrypted data are used, traffic analysis can also lead to attacks by cryptanalysis, whereby the attacker may obtain information or succeed in unencrypting the traffic.

Unit 1 Nishant Doshi

88

Click to add notes

SLIDE 88 OF 96 ENGLISH (INDIA)

Type here to search

NOTES COMMENTS

13:39 09-02-2024

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Shape Fill Shape Outline Quick Styles Shape Effects

Find Replace Select

Click to add title

• **Sniffing (man-in-the-middle)**: the attacker simply listens to messages exchanged by two entities. For the attack to be useful, the traffic must not be encrypted. Any unencrypted information, such as a password sent in response to an HTTP request, may be retrieved by the attacker.

• **Traffic analysis**: the attacker looks at the metadata transmitted in traffic in order to deduce information relating to the exchange and the participating entities, e.g. the form of the exchanged traffic (rate, duration, etc.). In the cases where **encrypted data** are used, traffic analysis can also lead to attacks by **cryptanalysis**, whereby the attacker may obtain information or succeed in unencrypting the traffic.

• **Software Attacks**: Malicious code (sometimes called *malware*) is a type of software designed to take over or damage a computer user's operating system, without the user's knowledge or approval. It can be very difficult to remove and very damaging.

[No Title]

Click to add notes

Unit 1 Nishant Doshi 89

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Layout Reset

Clipboard Slides

Font Paragraph

Drawing Editing

Find Replace Select

19

Software Attacks: Malicious code (sometimes referred to as viruses) is a type of software designed to take over or damage a computer user's operating system, without the user's knowledge or approval. It can be very difficult to remove and very damaging.

20

Need of Security policies-

- It increases efficiency.
- It upholds discipline and accountability
- It can make or break a business deal
- It helps to educate employees on security literacy

91

Virus and Spyware Protection policy:

- It helps to detect threats or files, to detect applications that exhibit suspicious behavior.
- Removes, and repairs the side effects of viruses and security risks by using signatures.

92

Firewall Policy:

- Blocks the unauthorized users from accessing the systems and networks that connect to the Internet.
- It detects the attacks by cybercriminals and removes the unwanted sources of network traffic.

93

Click to add title

Click to add notes

Unit 1 Nishant Doshi 90

The screenshot shows a Microsoft PowerPoint presentation titled 'Unit 1.pptx'. The slide has a blue header bar with the title 'Click to add title'. Below the header, there is a bulleted list under the heading 'Need of Security policies-'. The list includes: 'It increases efficiency.', 'It upholds discipline and accountability', 'It can make or break a business deal', and 'It helps to educate employees on security literacy'. To the left of the main slide, there are four smaller preview windows labeled 19, 20, 91, and 92, each containing a different slide content related to security policies. The bottom of the screen shows the PowerPoint ribbon tabs and a status bar indicating 'Unit 1 Nishant Doshi 90'.

Unit 1.pptx - PowerPoint

Ashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste New Slide Section Reset Layout Font Paragraph Drawing Editing

Clipboard Slides

98

89

★ Software Attacks: Malicious code (sometimes called malware) is a type of software designed to take over or damage a computer user's operating system, without the user's knowledge or approval. It can be very difficult to remove and very damaging.

90

★ Need of Security policies:

- It increases efficiency
- It upholds discipline and accountability
- It can make or break a business deal
- It helps to educate employees on security literacy

91

★ Virus and Spyware Protection policy:

- It helps to detect threads in files, to detect applications that exhibits suspicious behavior.
- Removes, and repairs the side effects of viruses and security risks by using signatures.

92

★ Firewall Policy:

- It blocks the unauthorized users from accessing the systems and networks that connect to the internet.
- It detects the attacks by cybercrimials and removes the unwanted sources of network traffic.

93

Click to add title

• **Virus and Spyware Protection policy:**

- It helps to detect threads in files, to detect applications that exhibits suspicious behavior.
- Removes, and repairs the side effects of viruses and security risks by using signatures.

Unit 1 Nishant Doshi 91

Click to add notes

Unit 1.pptx - PowerPoint

Aashka R.

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Clipboard Slides very damaging.

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Shapes Quick Styles Shape Effects

Find Replace Select

90 ★

• Need of Security policies:

- It increases efficiency.
- It upholds discipline and accountability.
- It can make or break a business deal.
- It helps to educate employees on security literacy.

91 ★

• Virus and Spyware Protection policy:

- It helps to detect threats or files, to detect applications that exhibit suspicious behavior.
- Removes, and repairs the side effects of viruses and security risks by using signatures.

92 ★

• Firewall Policy:

- It blocks the unauthorized users from accessing systems and networks that connect to the Internet.
- It detects the attacks by cybercriminals and removes the unwanted sources of network traffic.

93 ★

• Intrusion Prevention policy:

- This policy automatically detects and blocks the network attacks and browser attacks.
- It also protects applications from vulnerabilities and checks the contents of one or more data packages and detects malware which is coming through legal ways.

Click to add title

● **Firewall Policy:**

- 
- **It blocks the unauthorized users from accessing the systems and networks that connect to the Internet.**
- **It detects the attacks by cybercriminals and removes the unwanted sources of network traffic.**

Unit 1 Nishant Doshi

92

Click to add notes

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste New Slide Section Clipboard Slides Font Paragraph Drawing Editing

Aashka R

91

+ Virus and Spyware Protection policy:  
- It helps to detect threats in files, to protect applications that exhibits suspicious behavior.  
- Removes, and removes the side effects of viruses and removes risks by using signatures.

92

+ Firewall Policy:  
- It blocks the unauthorized users from accessing the systems and instances that connect to the Internet.  
- It detects the attacks by cyber criminals and removes the unwanted sources of network traffic.

93

+ Intrusion Prevention policy:  
- This policy automatically detects and blocks network attacks and browser attacks.  
- It also protects applications from vulnerabilities and checks the contents of one or more data packages and detects malware which is coming through legal ways.

94

+ Application and Device Control:  
- This policy protects a system's resources from applications and manages the peripheral devices that can attach to a system.  
- The device control policy applies to both Windows and mobile phones application control policy can be applied only to Windows clients.

Click to add title

● **Intrusion Prevention policy:**

- This policy automatically detects and blocks the network attacks and browser attacks.
- It also protects applications from vulnerabilities and checks the contents of one or more data packages and detects malware which is coming through legal ways.

Unit 1 Nishant Doshi

93

Click to add notes

NOTES COMMENTS

Unit 1.pptx - PowerPoint

Aashka R

Cut Copy Format Painter Paste New Slide Section Layout Reset Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Fill Shape Outline Shape Effects

Find Replace Select

93

Intrusion Prevention policy:

- This policy automatically detects and blocks the network attacks and incoming attacks.
- It also protects applications from vulnerabilities and checks the contents of one or more data packages and detects malware which is coming through legal way.

94

Application and Device Control:

- This policy protects a system's resources from applications and manages the peripheral devices that can attach to a system.
- The device control policy applies to both Windows and Mac computers whereas application control policy can be applied only to Windows clients.

95

References

- PPPU Syllabus
- NPTEL
- MIT
- Any other relevant material

96

Unit 1 Nishant Doshi

94

Click to add notes

Unit 1.pptx - PowerPoint

Aashka R -

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste New Slide Section Clipboard Slides

Font Paragraph

Drawing Editing

Find Replace Select

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Effects

Shape Fill Shape Outline

13 \* **Intrusion Prevention policy:**

- This policy automatically detects and blocks the network attacks and viruses.
- It also scans applications from vulnerabilities and checks the contents of one or more static packages and detects malware which is coming through legal ways.

34 \* **Application and Device Control:**

- This policy protects a system's resources from applications and manages the peripheral devices that can attach to a system.
- The application control policy applies to both Windows and Mac computers whereas application control policy can be applied only to Windows clients.

95 \* **References**

- PDPU Syllabus
- NPTEL
- MIT
- Any other relevant material

96 \* Click to add notes

Unit 1 Nishant Doshi

NOTES COMMENTS

The screenshot shows a Microsoft PowerPoint slide titled "References". The slide content is as follows:

## References

- PDPU Syllabus
- NPTEL
- MIT
- Any other relevant material

The slide is part of a presentation named "Unit 1.pptx". The ribbon at the top shows tabs for FILE, HOME, INSERT, DESIGN, TRANSITIONS, ANIMATIONS, SLIDE SHOW, REVIEW, and VIEW. The HOME tab is selected. The ribbon also includes sections for Font, Paragraph, Drawing, and Editing. On the left side of the slide, there are three callout boxes with star icons, each containing a different policy description. The bottom of the slide has a "Click to add notes" placeholder and a navigation bar with buttons for NOTES and COMMENTS.

Unit 1.pptx - PowerPoint

Aashka R -

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste

Clipboard Slides

Layout New Slide Section Reset

Font

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Effects

Drawing Select

Editing

93

★

- **Intrusion Prevention policy:**
  - This policy automatically detects and blocks the network attacks and intrusions attacks.
  - It also protects applications from vulnerabilities and checks the contents of one or more data packages and detects malware which is entering through legal ways.

94

★

- **Application and Device Control:**
  - This policy protects a system's resources from unauthorized access and manages the peripheral devices that are attached to the system.
  - The device control policy applies to both Windows and Mac computers whereas application control policy can be applied only to Windows clients.

95

★

References

- PDCU Syllabus
- NPTEL
- MIT
- Any other relevant material

96

★

Click to add notes

Click to add title

Sort1

N	Best case			Average Case			Worst Case		
	COMP	EXCH	TIME	COMP	EXCH	TIME	COMP	EXCH	TIME
10	#	#	#						
100									
1000									
10000									
100000									

Unit 1 Nishant Doshi

96

NOTES COMMENTS