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

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Aashka R

Cut Copy Format Painter Paste — Clipboard

New Slide Layout Reset Section — Slides

Font — Paragraph — Drawing — Editing

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Fill Shape Outline 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 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.

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.
- 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

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.

Unit 1 Nishant Doshi

Click to add notes

SLIDE 5 OF 96 ENGLISH (INDIA)

Type here to search

NOTES COMMENTS

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste Clipboard

New Slide Layout Reset Section Slides

Font

Text Direction Align Text Convert to SmartArt Paragraph

Arrange Quick Styles Shape Fill Shape Outline Shape Effects Drawing

Find Replace Select Editing

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 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.

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.
- 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

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.

Unit 1 Nishant Doshi

Click to add notes

NOTES COMMENTS

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.

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 Clipboard

New Slide Layout Reset Section Slides

Font Paragraph

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Fill Shape Outline Shape Effects Drawing

Find Replace Select Editing

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.
- 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 modifying the features of a computer and software, or computer data, to accomplish a goal outside of the creator's original purpose.
- 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 Java or another 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 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.

9 Types of Hacking

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.

Click to add notes

NOTES COMMENTS 85%

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.

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 Clipboard

New Slide Layout Reset Section Slides

Font Paragraph

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Fill Shape Outline Shape Effects Drawing

Find Replace Select Editing

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, tampering the Uniform Resource Identifier (URI) or tampering HTTP elements not contained in the URI.

10 [No Title]

- **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 key-logging.

Password:

12

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

SOCIAL ENGINEERING

13

Click to add title

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

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 Layout Reset 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

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, tampering the Uniform Resource Identifier (URI) or tampering HTTP elements not contained in the URI.

10

- **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 key-logging.

12

- **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

HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter | New Slide Layout Reset Section | Text Direction Align Text Convert to SmartArt | Arrange Quick Styles Shape Fill Shape Outline Shape Effects | Find Replace Select

Clipboard Slides Font Paragraph Drawing Editing

1 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.

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

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

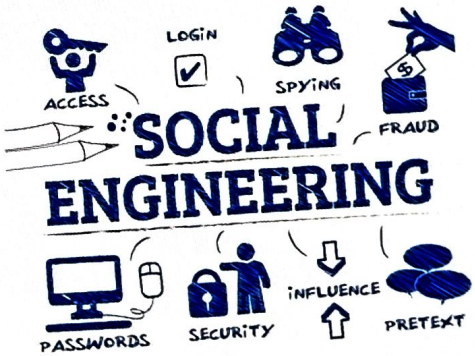
Password:

12 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

- **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

[No Title]

NOTES COMMENTS 85%

Unit 1.pptx - PowerPoint

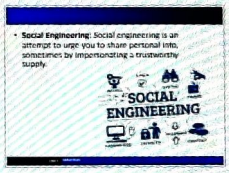
Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

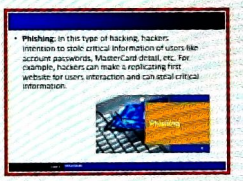
Paste Cut Copy Format Painter | New Slide Layout Reset Section | Text Direction Align Text Convert to SmartArt | Arrange Quick Styles Shape Fill Shape Outline Shape Effects | Find Replace Select

Clipboard Slides Font Paragraph Drawing Editing

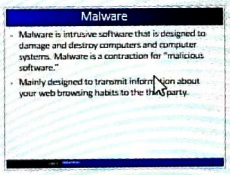
12



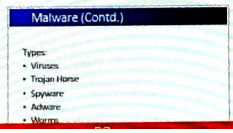
13



14



15



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.

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 Paste

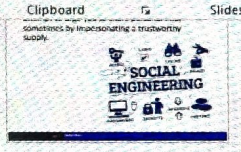
Layout Reset Section New Slide

Text Direction Align Text Convert to SmartArt

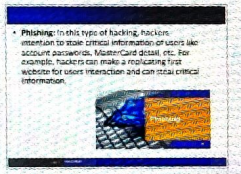
Shape Fill Shape Outline Shape Effects Arrange Quick Styles

Find Replace Select

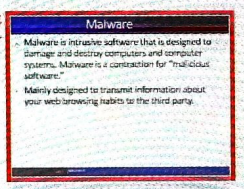
Clipboard Slides Font Paragraph Drawing Editing



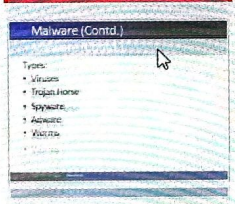
13



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

Unit 1.pptx - PowerPoint

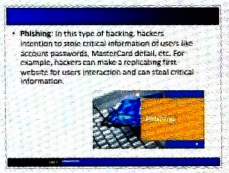
Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

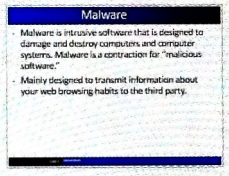
Paste Cut Copy Format Painter | New Slide Layout Reset Section | Clipboard Slides Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt | Arrange Quick Styles | Shape Fill Shape Outline Shape Effects | Find Replace Select

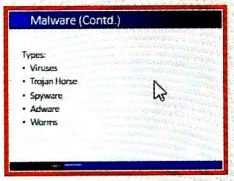
13



14



15



16

Malware (Contd.)

Types:

- Viruses
- Trojan Horse
- Spyware
- Adware
- Worms

Unit 1 Nishant Doshi

Click to add notes

SLIDE 15 OF 96 ENGLISH (INDIA)

NOTES COMMENTS 85%

Type here to search

ENG 13:36 09-02-2024

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste — Clipboard

New Slide Layout Reset Section — Slides

Font — Paragraph — Drawing — Editing

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Fill Shape Outline Shape Effects

Find Replace Select

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 (World Summit on the Information Society) Proposed the definition.

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.

INTERNET GOVERNANCE

- WSIS (World Summit on the Information Society) Proposed the definition.

WSIS FORUM 2023

Unit 1 Nishant Doshi

Click to add notes

85%

Unit 1.pptx - PowerPoint

DRAWING TOOLS

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW FORMAT

Paste Cut Copy Format Painter | New Slide Layout Reset Section | Calibri (Body) 32 | Text Direction Align Text Convert to SmartArt | Arrange Quick Styles Shape Fill Shape Outline Shape Effects | Find Replace Select

Clipboard Slides Font Paragraph Drawing Editing

15 Malware (Contd.)

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

16 INTERNET GOVERNANCE

- WSIS (World Summit on the Information Society) Proposed the definition.

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. 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.

INTERNET GOVERNANCE

19 SELF REGULATION

- Self regulation works in a group with strong

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.

Unit 1 Nishant Doshi

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

NOTES COMMENTS 85%

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste Clipboard

New Slide Layout Reset Section Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Shape Fill Shape Outline Shape Effects Arrange Quick Styles

Find Replace Select

15 Malware (Contd.)

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

16 INTERNET GOVERNANCE

WSIS FORUM 2023

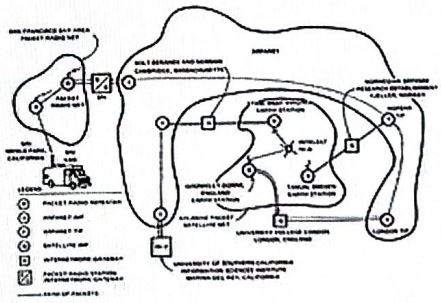
17 INTERNET GOVERNANCE

18 INTERNET GOVERNANCE

19 SELF REGULATION

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.



Click to add text

Unit 1 Nishant Doshi

Click to add notes

SLIDE 18 OF 96 ENGLISH (INDIA)

NOTES COMMENTS 85%

Type here to search

ENG 13:37 09-02-2024

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste | Layout Reset New Slide Section | Text Direction Align Text Convert to SmartArt | Arrange Quick Styles Shape Fill Shape Outline Shape Effects | Find Replace Select

Clipboard Slides Font Paragraph Drawing Editing

17 INTERNET GOVERNANCE

18 INTERNET GOVERNANCE

19 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 thing 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

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 thing are managed automatically.

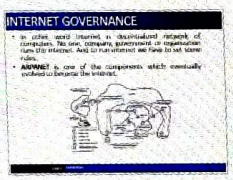
Click to add notes

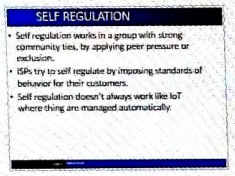
Unit 1.pptx - PowerPoint

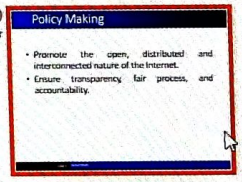
Aashka R

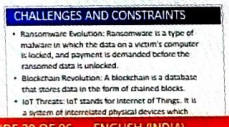
HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter | New Slide | Layout Reset Section | Clipboard Slides | Font | Text Direction Align Text Convert to SmartArt | Paragraph | Arrange Quick Styles Shape Fill Shape Outline Shape Effects | Drawing | Find Replace Select | Editing









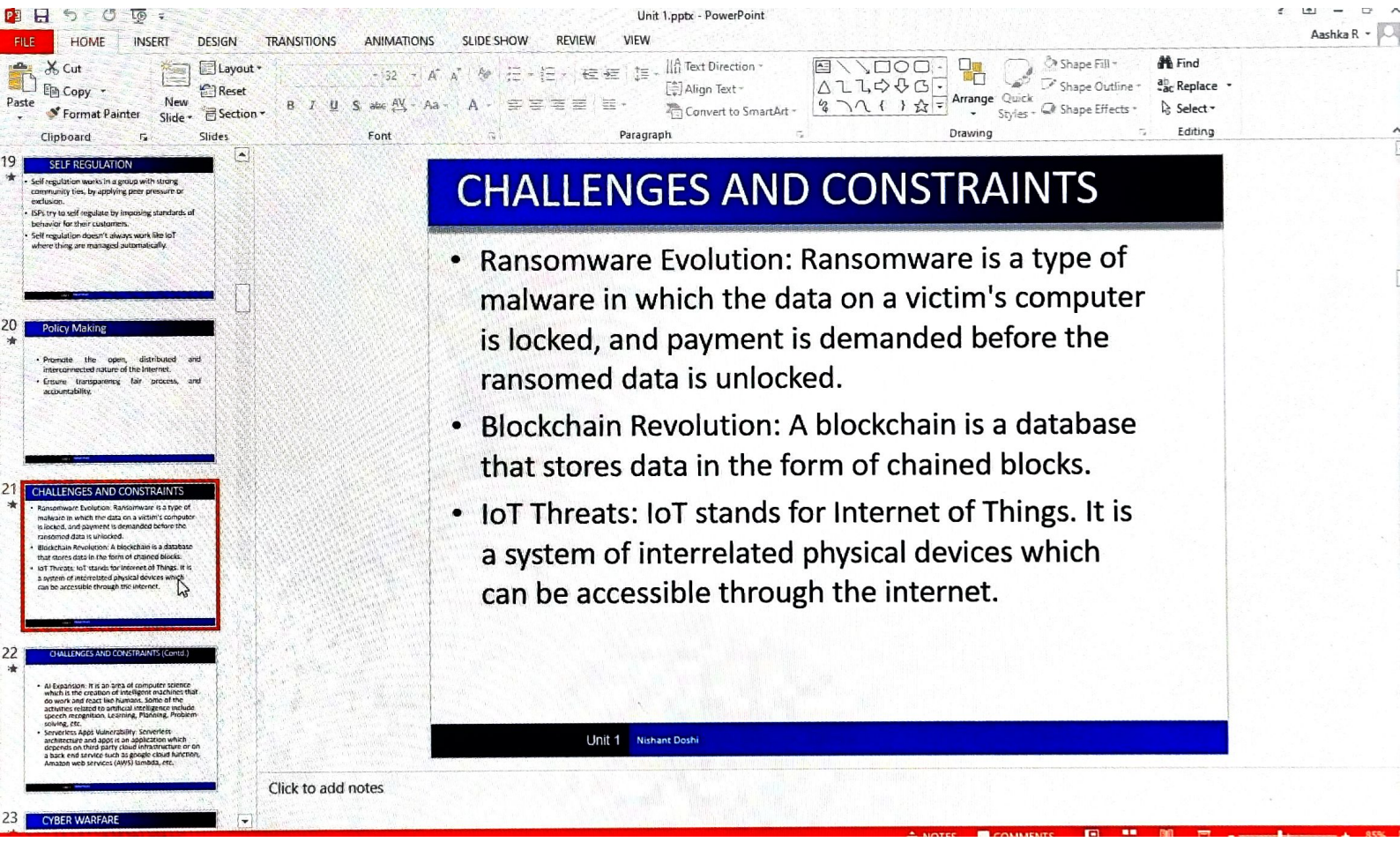
Policy Making

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

Unit 1 Nishant Doshi

Click to add notes

NOTES COMMENTS


Unit 1.pptx - PowerPoint
FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Aashka R
Cut
Copy
Format Painter
Paste
Clipboard
New Slide
Layout
Reset
Section
Slides
Font
Text Direction
Align Text
Convert to SmartArt
Paragraph
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Drawing
Find
Replace
Select
Editing
19
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 thing 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 activities related to artificial intelligence include speech recognition, Learning, Planning, Problem solving, etc.
• Serverless Apps Vulnerability: Serverless architecture and appt it 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.
23
CYBER WARFARE
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.
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

New Slide Layout Reset Section Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Fill Shape Outline Shape Effects

Find Replace Select

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 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 CONSTRAI...

23 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.

24 CYBER WARFARE Types

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.

Click to add notes

NOTES COMMENTS 85%

Unit 1.pptx - PowerPoint

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Aashka R

Paste Cut Copy Format Painter | New Slide Layout Reset Section | Text Direction Align Text Convert to SmartArt | Arrange Quick Styles Shape Fill Shape Outline Shape Effects | Find Replace Select

Clipboard Slides Font Paragraph Drawing Editing

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 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.

23 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.

CYBER WARFARE

24 CYBER WARFARE Types

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

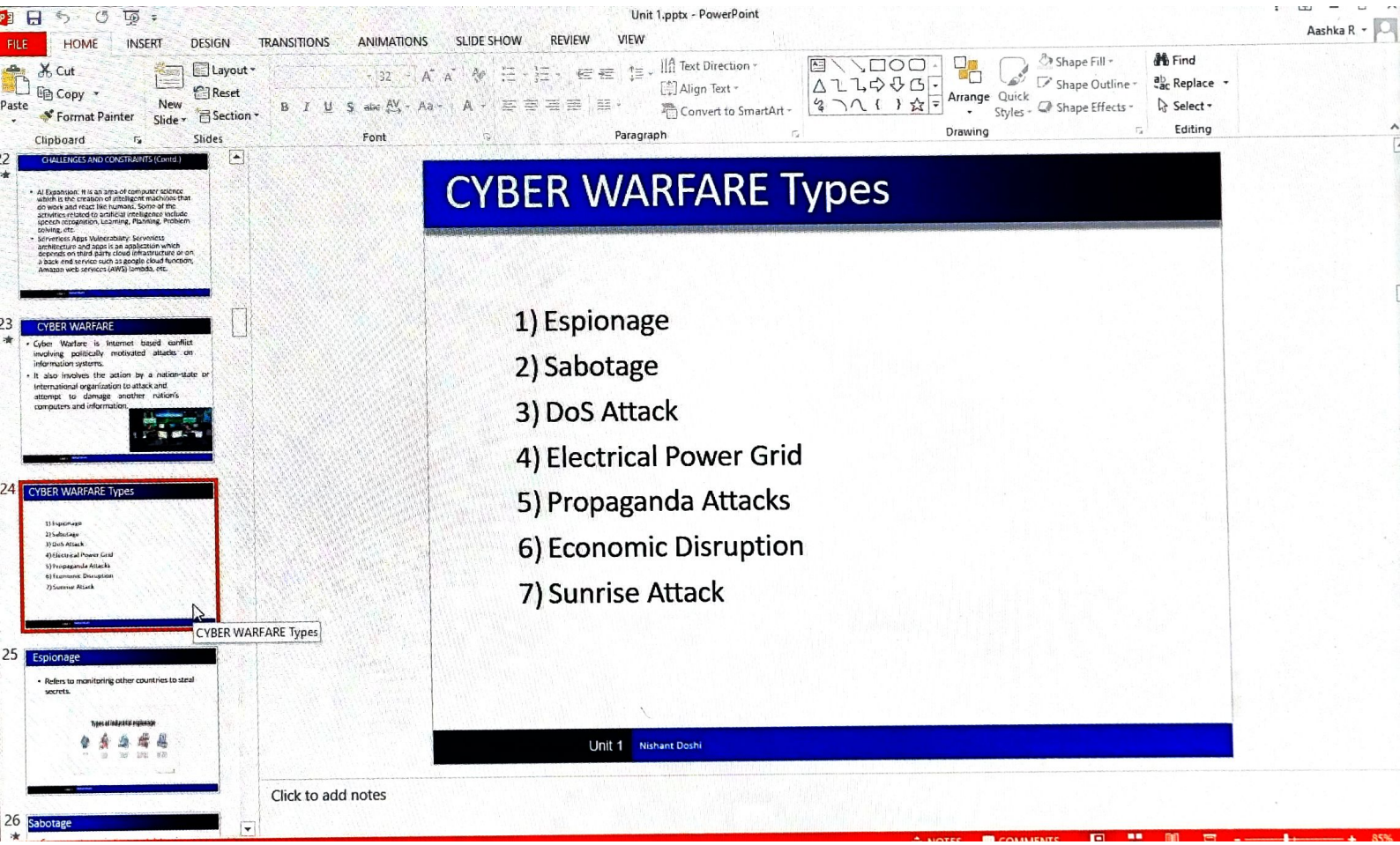
CYBER WARFARE

- 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 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
Paste
New Slide
Layout
Reset
Section
Clipboard
Slides
Font
Text Direction
Align Text
Convert to SmartArt
Paragraph
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Drawing
Find
Replace
Select
Editing
22
CHALLENGES AND CONSTRAINTS (Contd.)
23
CYBER WARFARE
24
CYBER WARFARE Types
25
Espionage
26
Sabotage
CYBER WARFARE Types
CYBER WARFARE Types
1) Espionage
2) Sabotage
3) DoS Attack
4) Electrical Power Grid
5) Propaganda Attacks
6) Economic Disruption
7) Sunrise Attack
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 Layout Reset Section

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Fill Shape Outline Shape Effects

Find Replace Select

Clipboard Slides Font Paragraph Drawing Editing

24 CYBER WARFARE Types

25 Espionage

- Refers to monitoring other countries to steal secrets.

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.

27 Sabotage (Contd.)

28 Denial of Service (DoS)

Espionage

- Refers to monitoring other countries to steal secrets.

Types of industrial espionage

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

Paste Cut Copy Format Painter | New Slide Layout Reset Section | Text Direction Align Text Convert to SmartArt | Arrange Quick Styles Shape Fill Shape Outline Shape Effects | Find Replace Select

Clipboard Slides Font Paragraph Drawing Editing

24 CYBER WARFARE Types

25 Espionage
- Refers to monitoring other countries to steal secrets.

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.

27 Sabotage (Contd.)

28 Denial of Service (DoS)

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.

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 Layout Reset Section

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Fill Shape Outline Shape Effects

Find Replace Select

Clipboard Slides Font Paragraph Drawing Editing

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

- 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.

27 Sabotage (Contd.)

28 Denial of Service (DoS)

Sabotage (Contd.)

Click to add notes

Unit 1.pptx - PowerPoint

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Aashka R

Paste Cut Copy Format Painter New Slide Layout Reset 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

26

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.

27 Sabotage (Contd.)

28 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.

29

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

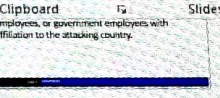
Unit 1.pptx - PowerPoint

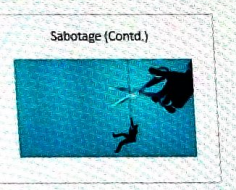
HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

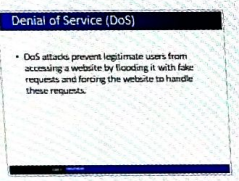
Aashka R

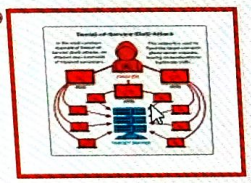
Cut Copy Format Painter | New Slide Layout Reset Section | Text Direction Align Text Convert to SmartArt | Arrange Quick Styles Shape Fill Shape Outline Shape Effects | Find Replace Select

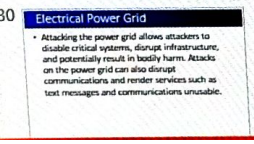
Clipboard Slides Font Paragraph Drawing Editing











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

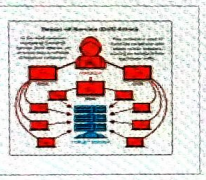
Unit 1.pptx - PowerPoint

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

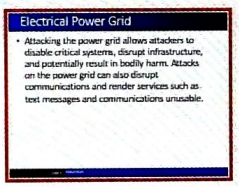
Aashka R

Cut Copy Format Painter Paste Layout Reset Section New Slide Clipboard Slides Font Paragraph Text Direction Align Text Convert to SmartArt Drawing Arrange Quick Styles Shape Fill Shape Outline Shape Effects Find Replace Select Editing

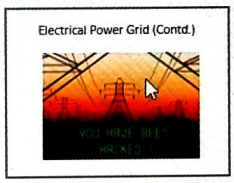
29



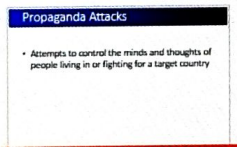
30



31



32



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.

Unit 1 Nishant Doshi

Click to add notes

Unit 1.pptx - PowerPoint

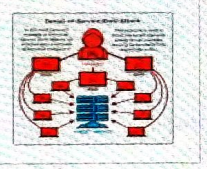
Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste | New Slide Layout Reset Section | Text Direction Align Text Convert to SmartArt | Arrange Quick Styles Shape Fill Shape Outline Shape Effects | Find Replace Select

Clipboard Slides Font Paragraph Drawing Editing

29



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.)

Electrical Power Grid (Contd.)

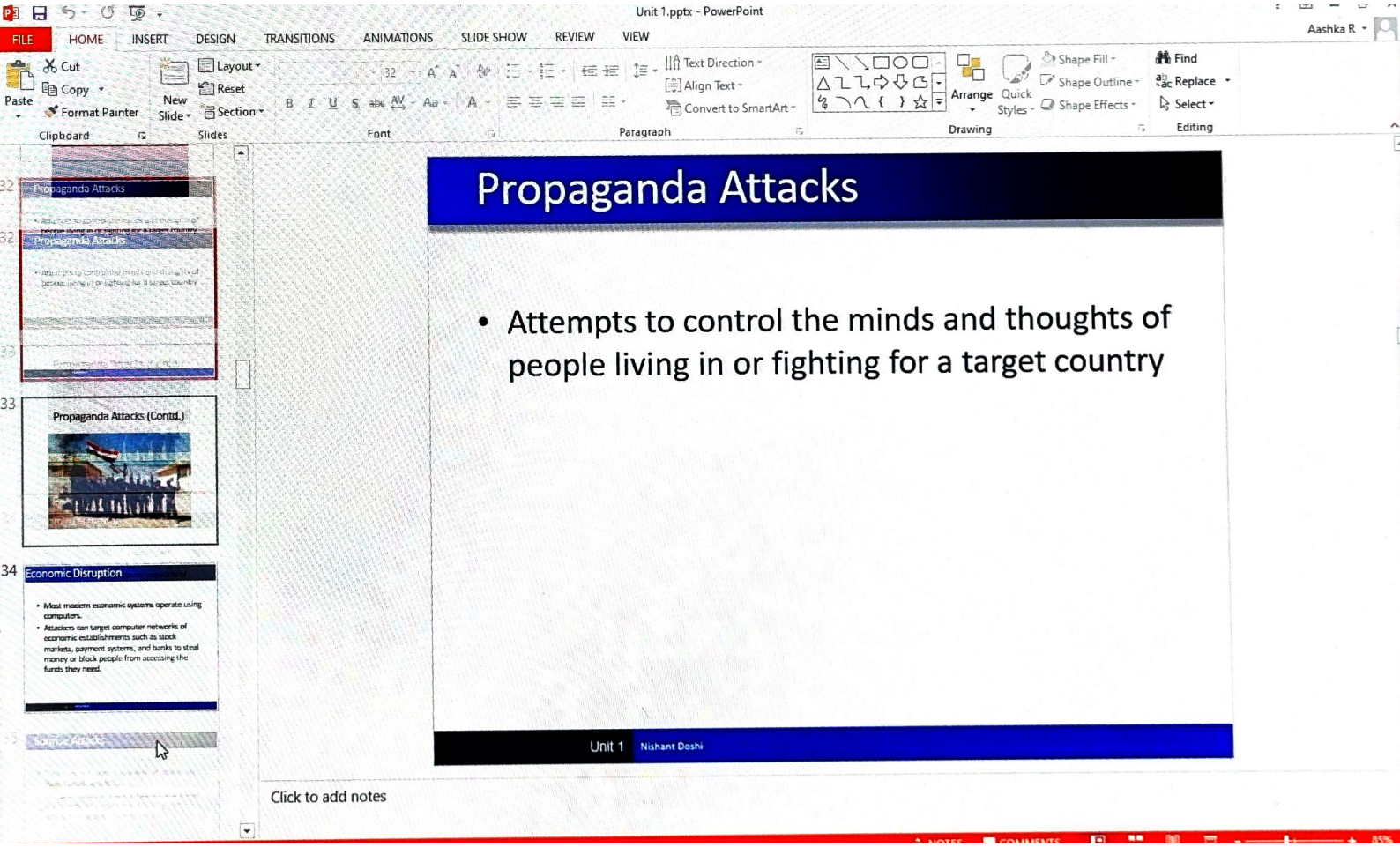
32

Propaganda Attacks

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

Electrical Power Grid (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
Layout
Reset
Section
Text Direction
Align Text
Convert to SmartArt
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Find
Replace
Select
Clipboard
Slides
Font
Paragraph
Drawing
Editing
32
Propaganda Attacks
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.
Propaganda Attacks
Attempts to control the minds and thoughts of people living in or fighting for a target country
Unit 1
Nishant Doshi
Click to add notes

Unit 1.pptx - PowerPoint

Aashka R

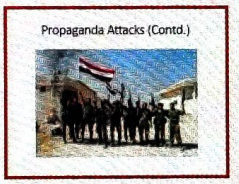
FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Paste Cut Copy Format Painter — Clipboard

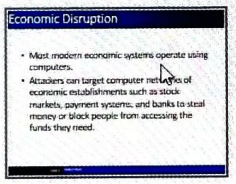
New Slide Layout Reset Section — Slides

Font — Paragraph — Text Direction Align Text Convert to SmartArt — Drawing — Arrange Quick Styles Shape Fill Shape Outline Shape Effects — Editing Find Replace Select

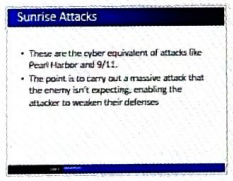
33



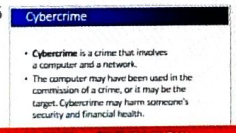
34



35



36



Propaganda Attacks (Contd.)

Click to add notes

NOTES COMMENTS

Unit 1.pptx - PowerPoint

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Aashka R

Paste Cut Copy Format Painter | New Slide Layout Reset Section | Text Direction Align Text Convert to SmartArt | Arrange Quick Styles Shape Fill Shape Outline Shape Effects | Find Replace Select

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.

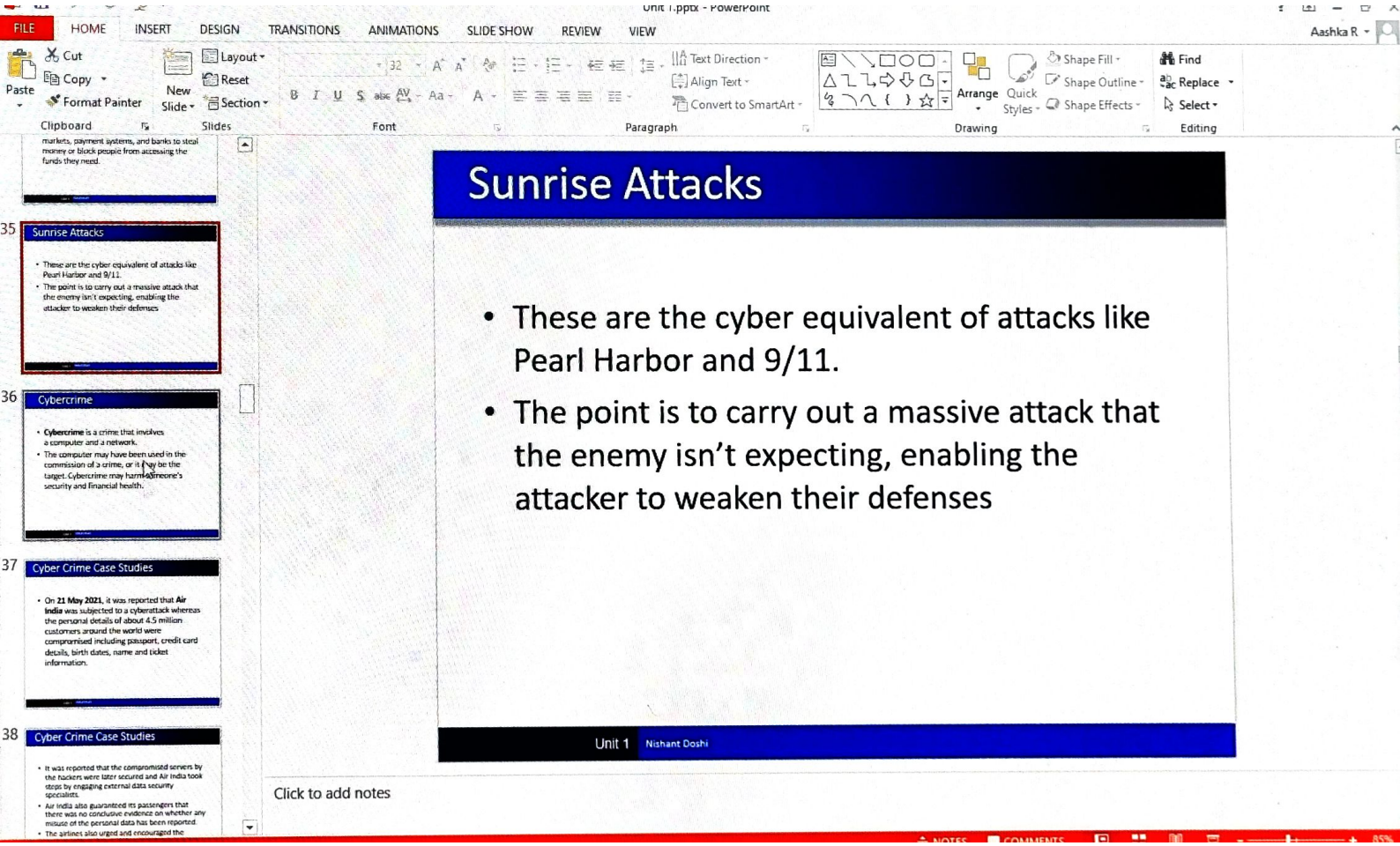
Economic Disruption

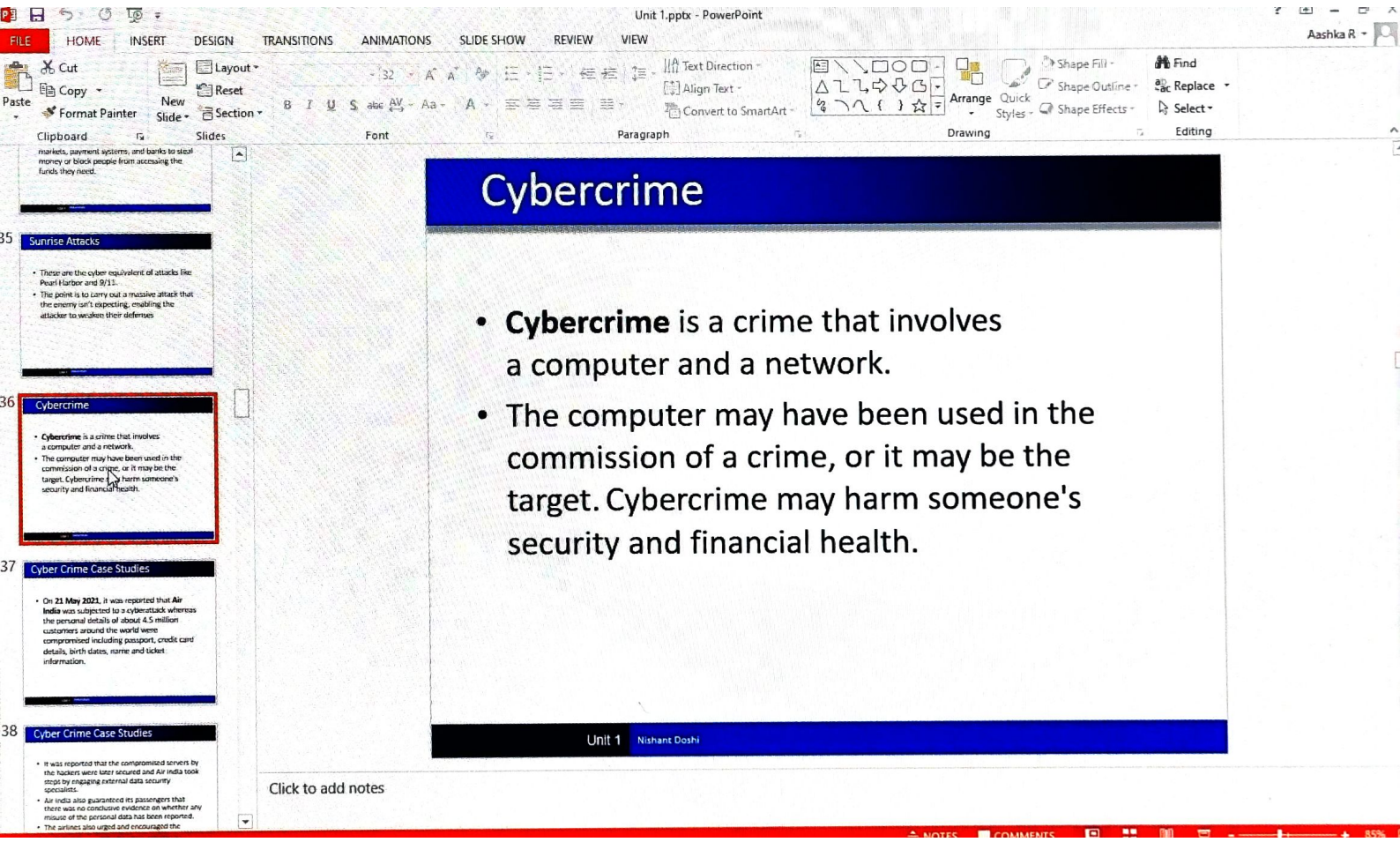
- Most modern economic systems operate using computers.
- Attackers can target computer networks of economic establishments such as stock markets, payment systems, and banks to steal money or block people from accessing the funds they need.

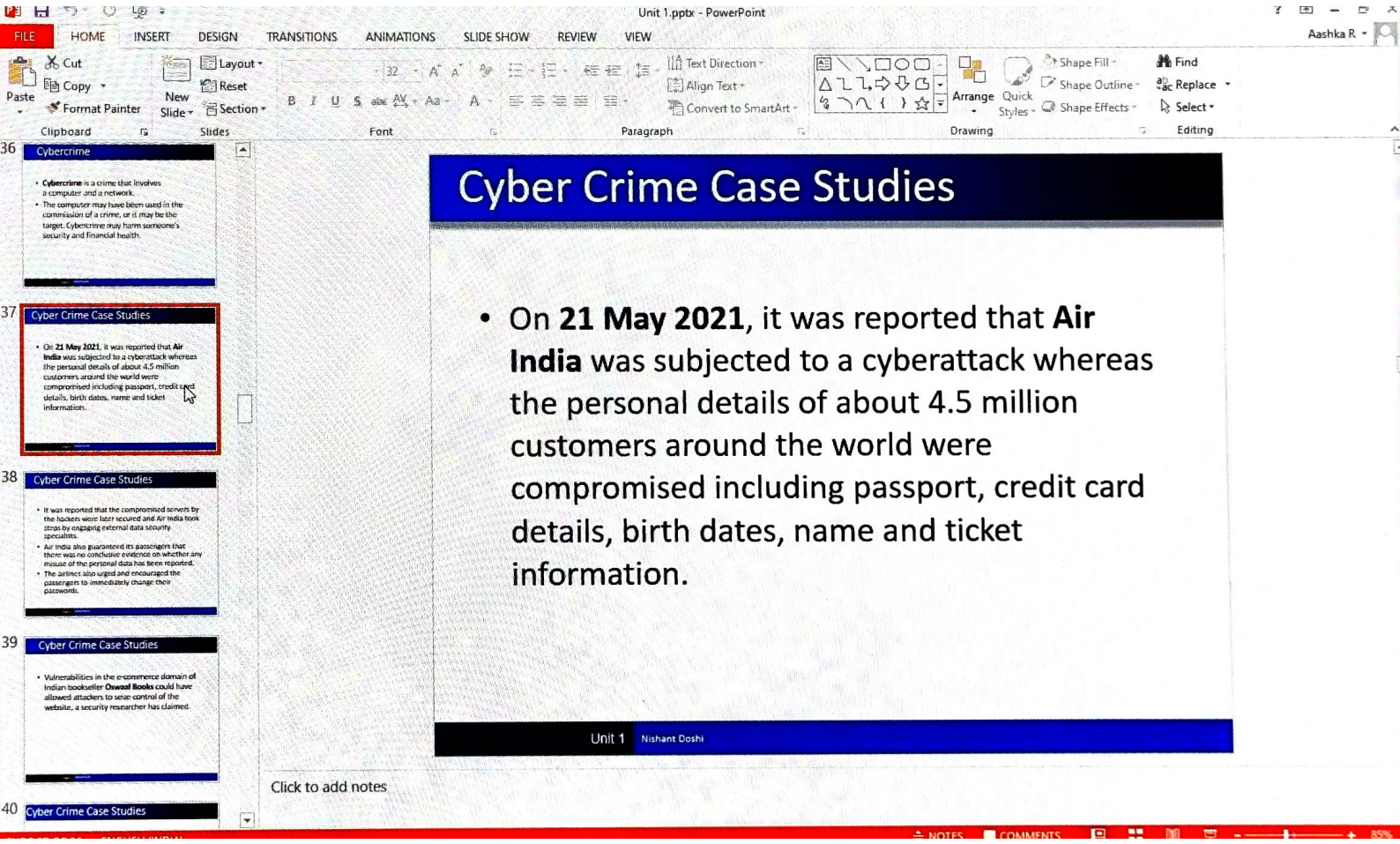
Unit 1 Nishant Doshi

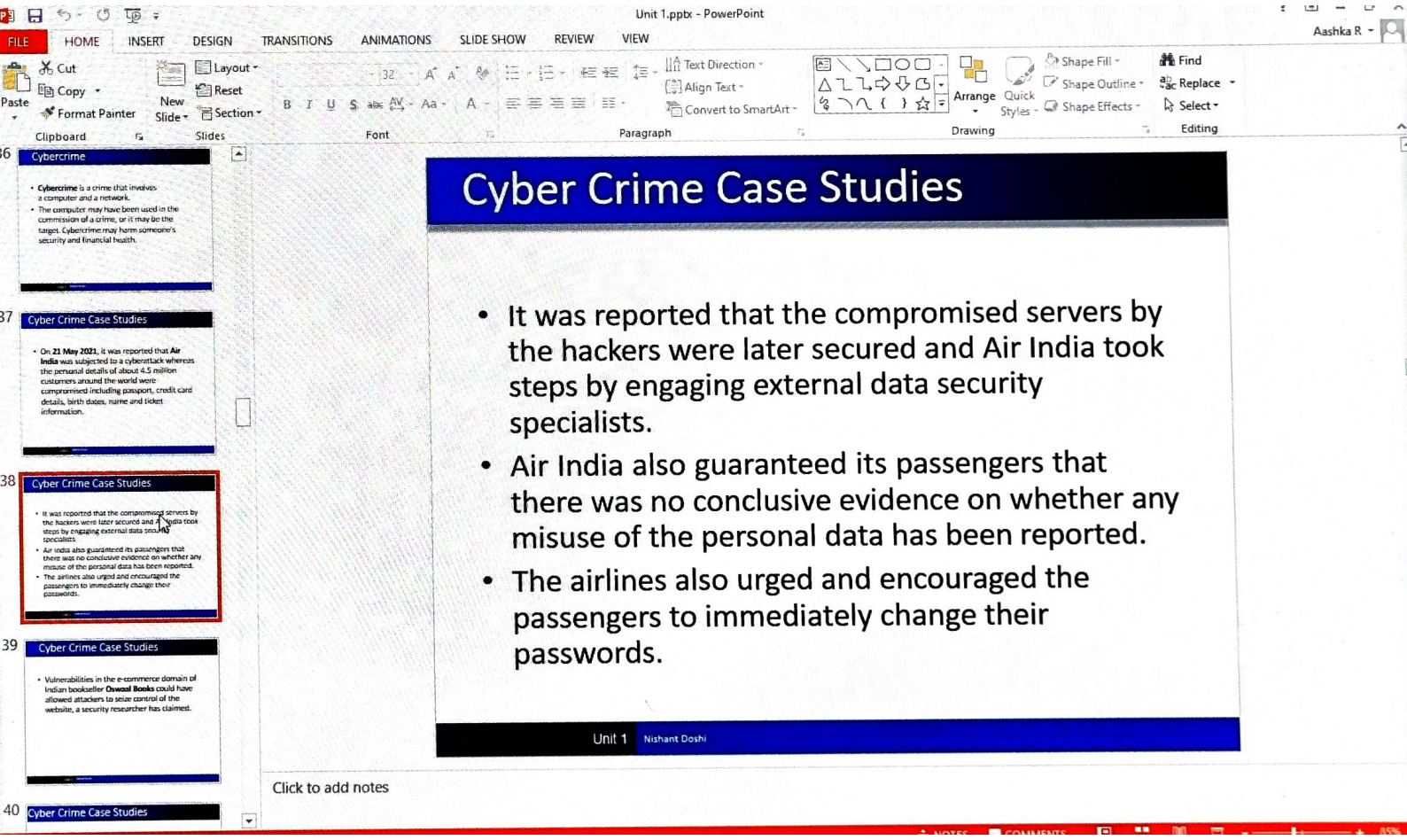
Click to add notes

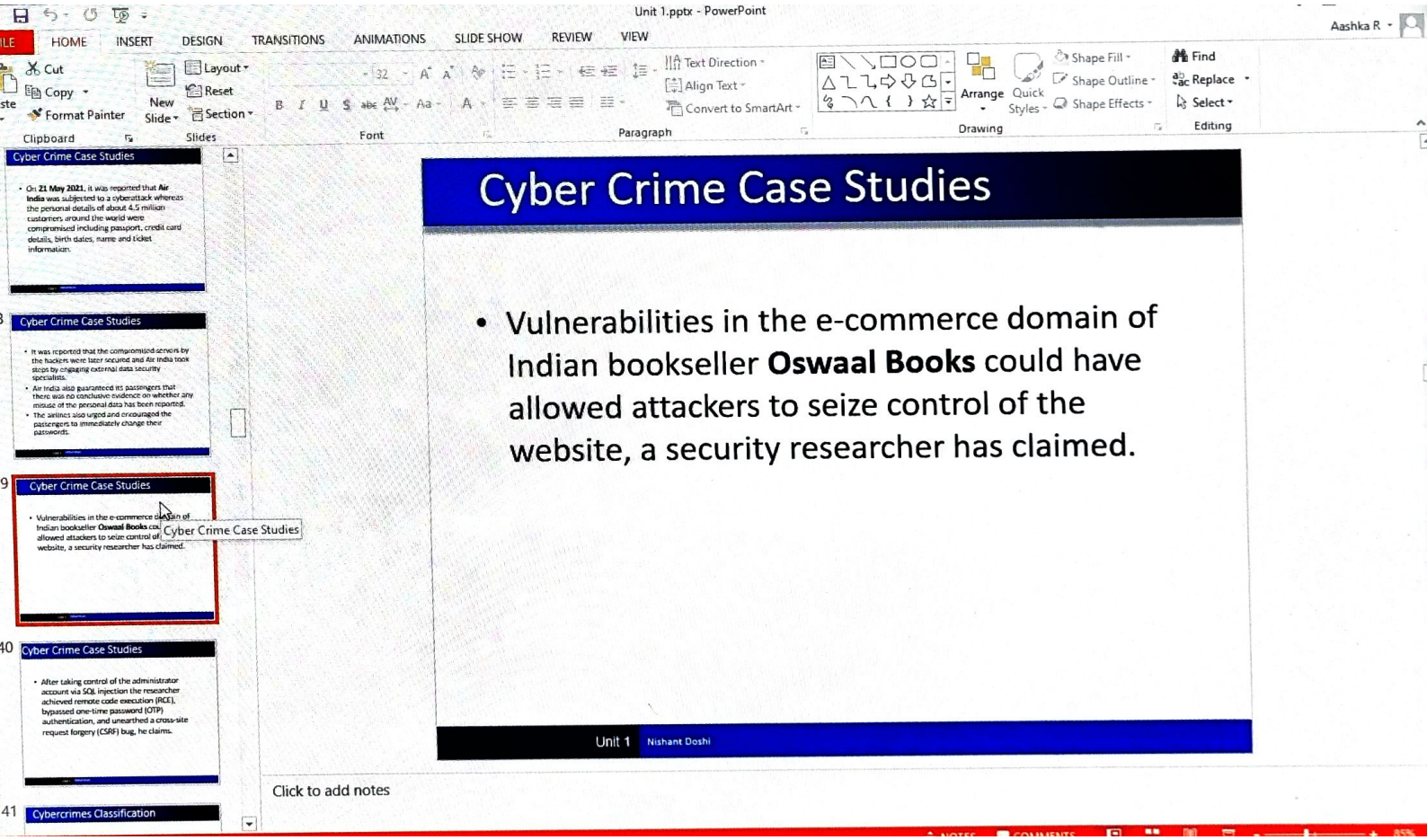
NOTES COMMENTS 85%

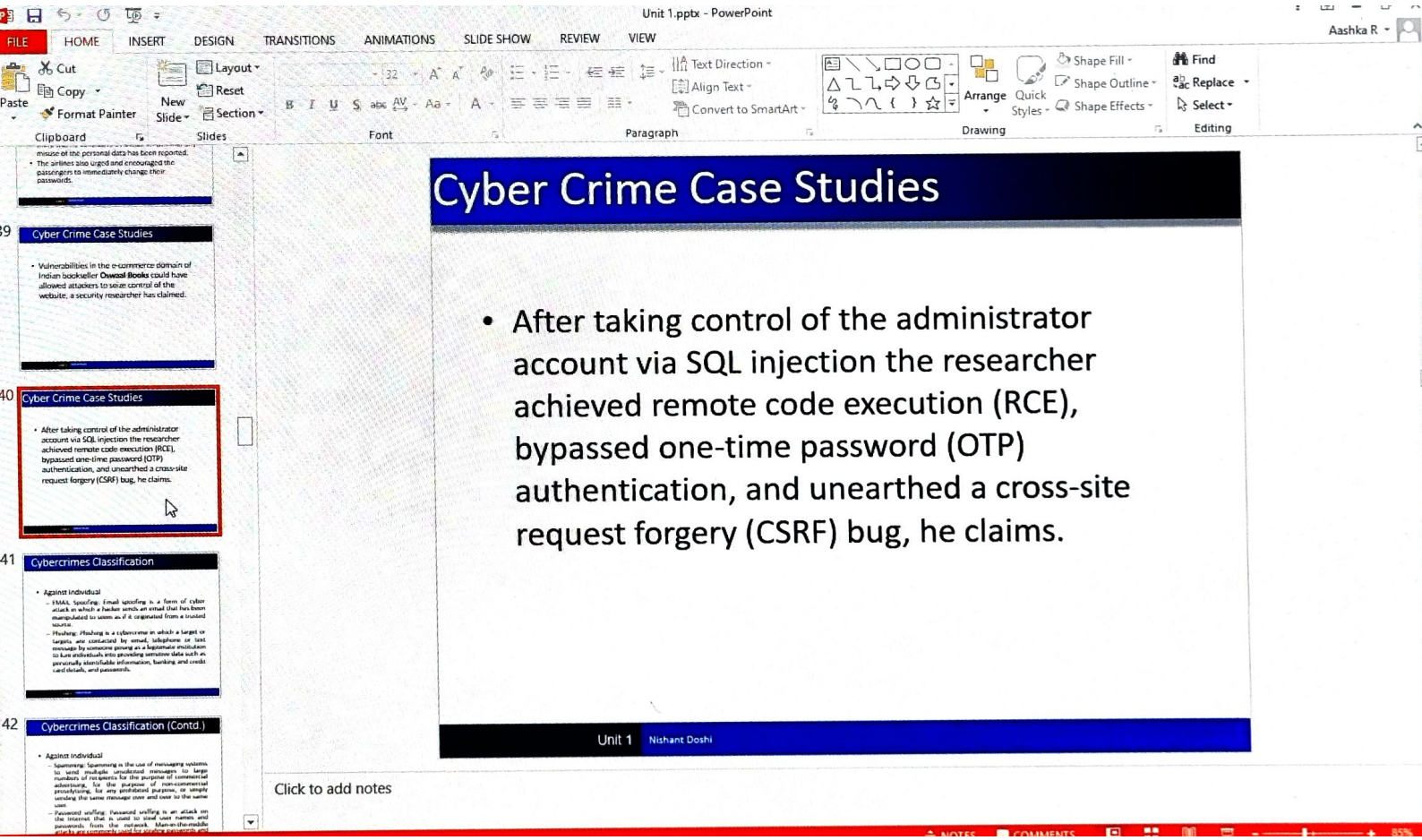

Unit 1.pptx - PowerPoint
FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Aashka R.
Cut
Copy
Format Painter
Paste
Clipboard
New Slide
Layout
Reset
Section
Slides
Font
Text Direction
Align Text
Convert to SmartArt
Paragraph
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Drawing
Find
Replace
Select
Editing
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.
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 reported.
• 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

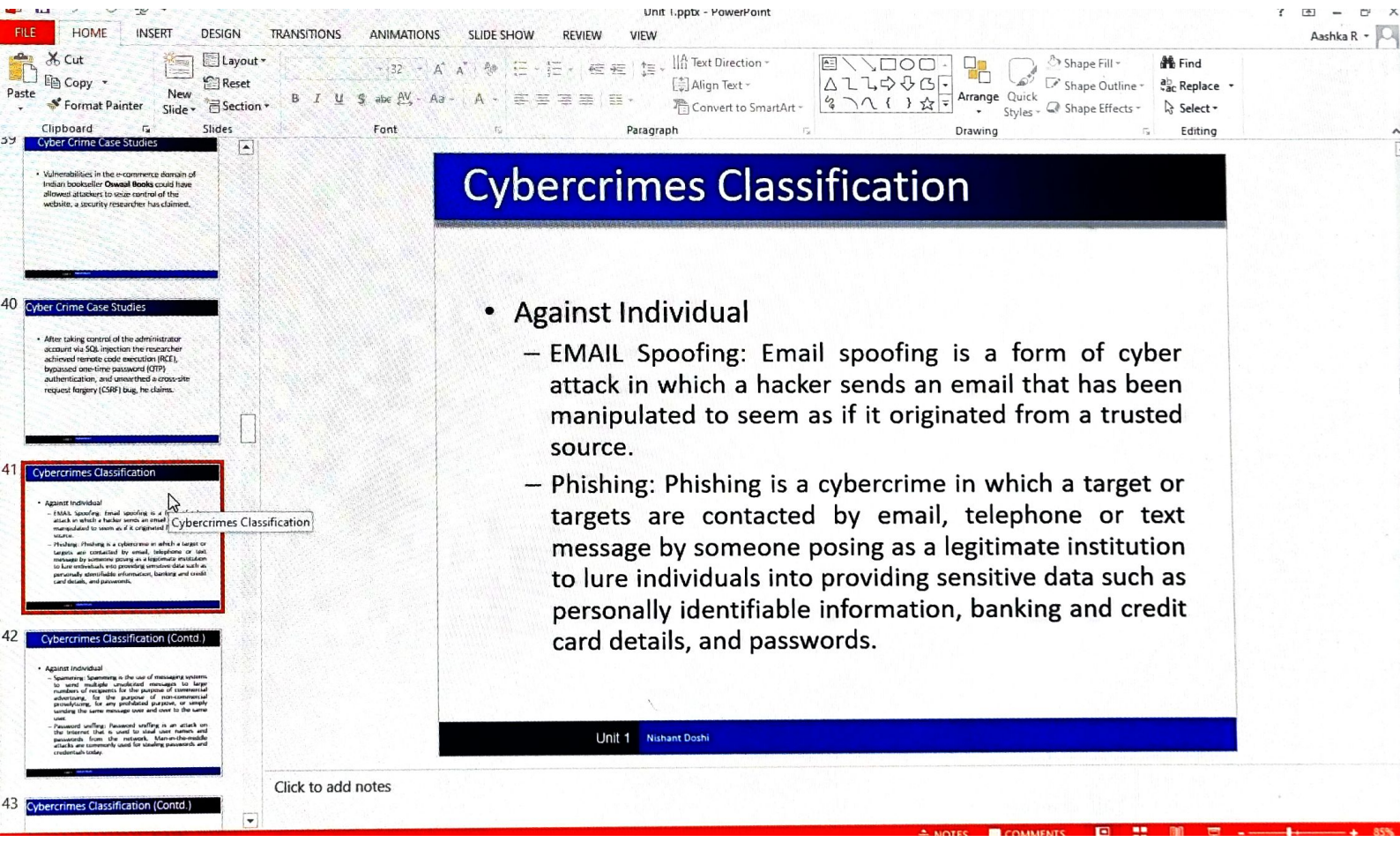

Unit 1.pptx - PowerPoint
FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Aashka R
Cut
Copy
Format Painter
Paste
New Slide
Layout
Reset
Section
Clipboard
Slides
Font
Text Direction
Align Text
Convert to SmartArt
Paragraph
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Drawing
Find
Replace
Select
Editing
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.
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 reported.
• The airlines also urged and encouraged the
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.
Unit 1
Nishant Doshi
Click to add notes
NOTES
COMMENTS

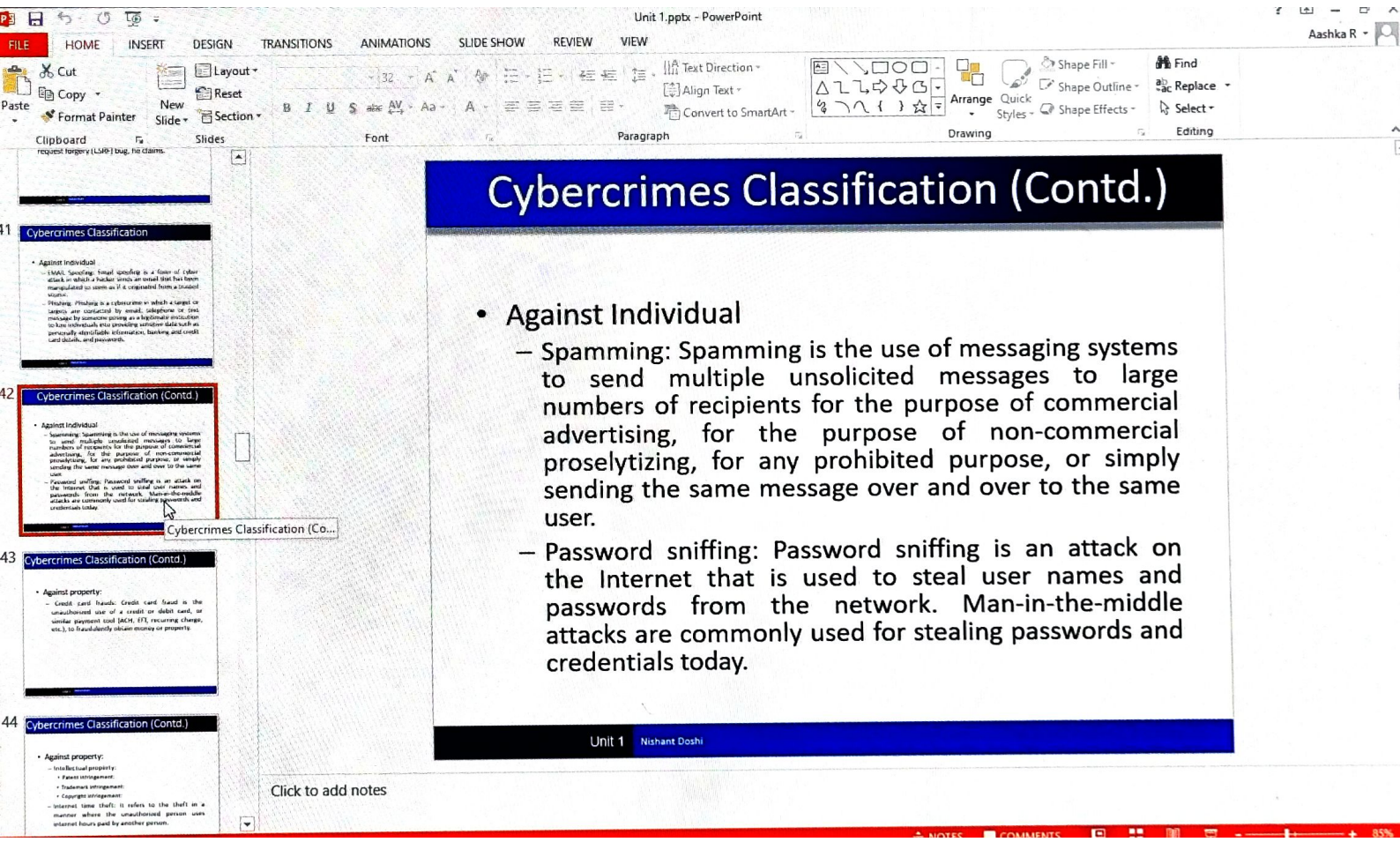

Unit 1.pptx - PowerPoint
FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Aashka R
Cut
Copy
Format Painter
Paste
New Slide
Layout
Reset
Section
Clipboard
Slides
Font
Text Direction
Align Text
Convert to SmartArt
Paragraph
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Drawing
Find
Replace
Select
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 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
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.
Unit 1
Nishant Doshi
Click to add notes
NOTES
COMMENTS

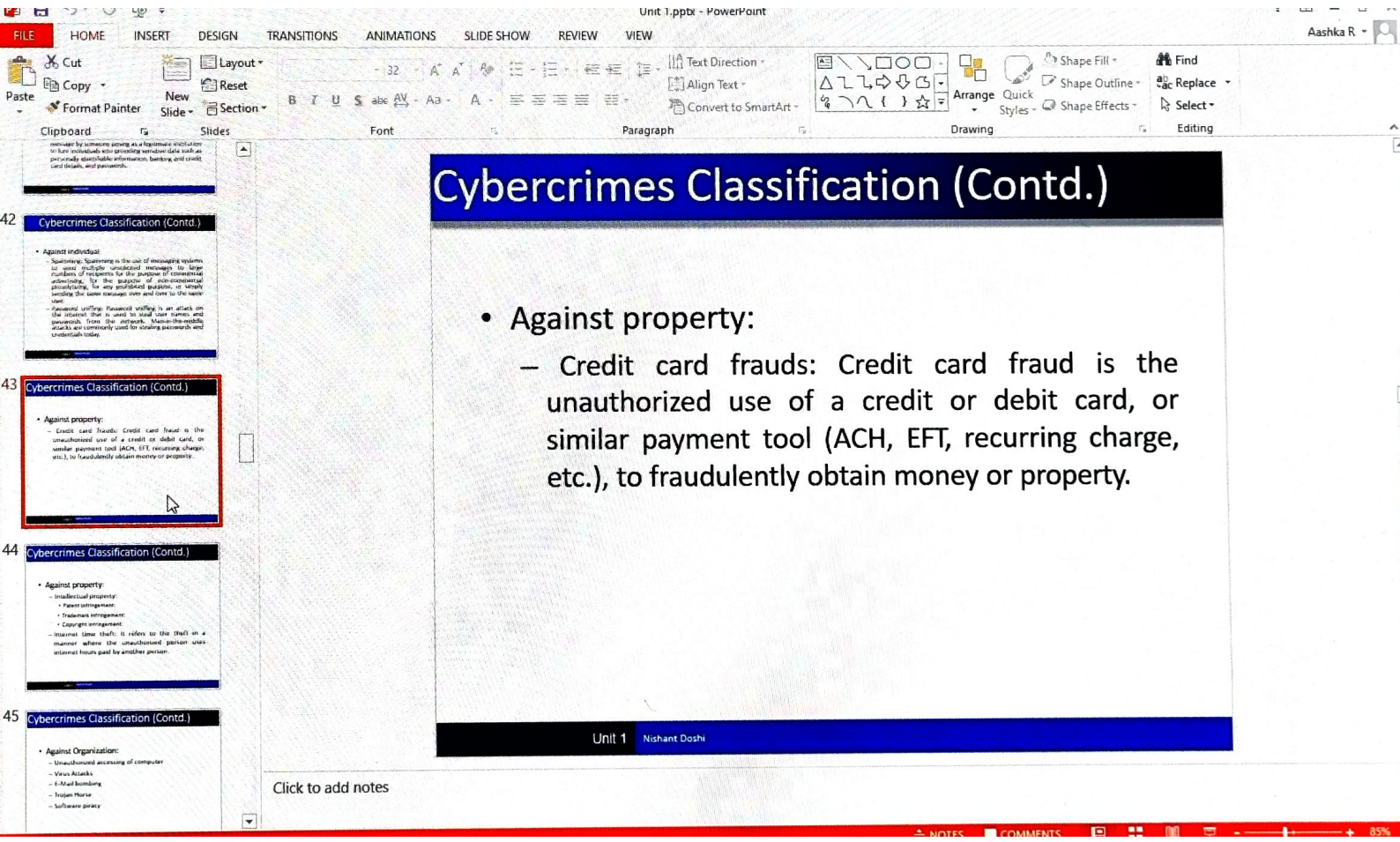

Unit 1.pptx - PowerPoint
Aashka R
FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Cut
Copy
Format Painter
Paste
New Slide
Layout
Reset
Section
Text Direction
Align Text
Convert to SmartArt
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Find
Replace
Select
Clipboard
Slides
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 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
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.
Unit 1
Nishant Doshi
Click to add notes

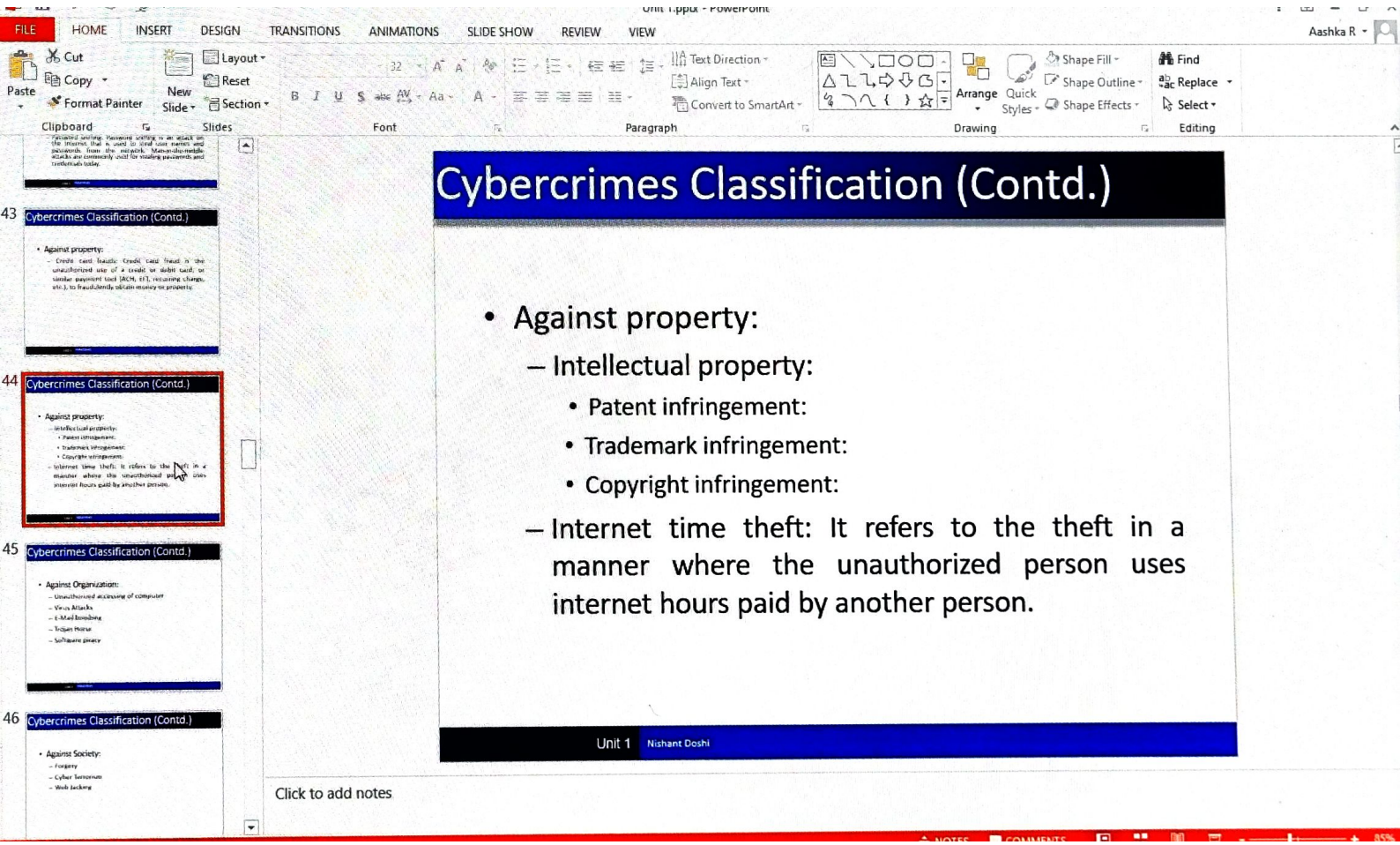

Unit 1.pptx - PowerPoint
Aashka R
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Cut
Copy
Format Painter
New Slide
Layout
Reset
Section
Text Direction
Align Text
Convert to SmartArt
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Find
Replace
Select
Clipboard
Slides
Font
Paragraph
Drawing
Editing
Cyber Crime Case Studies
Cyber Crime Case Studies
Cyber Crime Case Studies
Cyber Crime Case Studies
Cyber Crime Case Studies
Cybercrimes Classification
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.
Unit 1
Nishant Doshi
Click to add notes

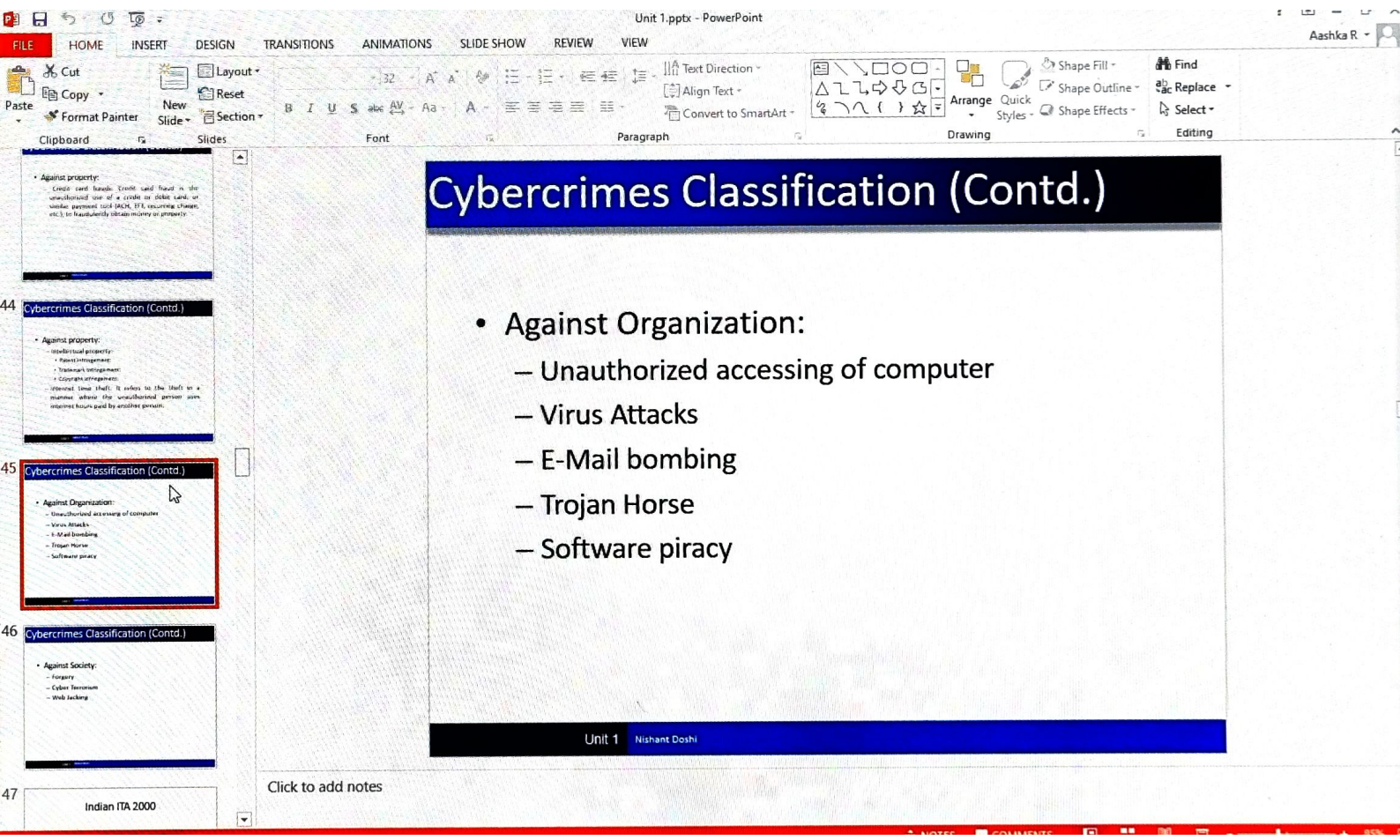

Unit 1.pptx - PowerPoint
Aashka R
FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Cut
Copy
Format Painter
Paste
Layout
Reset
New Slide
Section
Clipboard
Slides
Font
Text Direction
Align Text
Convert to SmartArt
Paragraph
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Drawing
Find
Replace
Select
Editing
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
Against Individual
Cybercrimes Classification (Contd.)
Against Individual
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

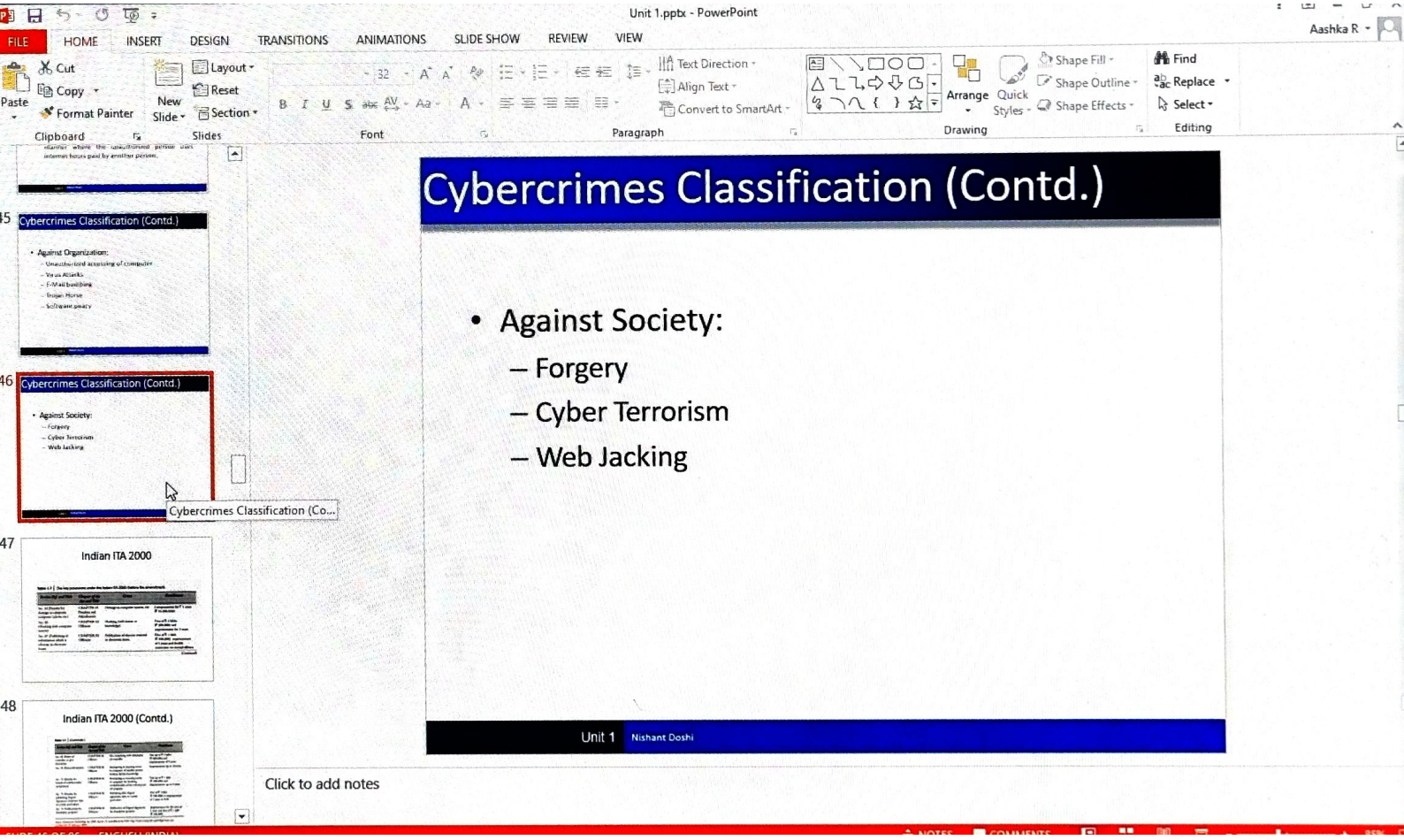

Unit 1.pptx - PowerPoint
FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Aashka R
Paste
Cut
Copy
Format Painter
New Slide
Layout
Reset
Section
Text Direction
Align Text
Convert to SmartArt
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Find
Replace
Select
Clipboard
Slides
Font
Paragraph
Drawing
Editing
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
• 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
attack in which a hacker sends an email
manipulated to seem as if it originated
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.
Cybercrimes Classification
42 Cybercrimes Classification (Contd.)
• Against Individual
– Spamming: Spamming 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.
43 Cybercrimes Classification (Contd.)
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.
Unit 1
Nishant Doshi
Click to add notes
NOTES
COMMENTS

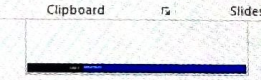

Unit 1.pptx - PowerPoint
Aashka R
FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Cut
Copy
Format Painter
Paste
New Slide
Layout
Reset
Section
Clipboard
Slides
Font
Paragraph
Drawing
Editing
Text Direction
Align Text
Convert to SmartArt
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Find
Replace
Select
41
Cybercrimes Classification
42
Cybercrimes Classification (Contd.)
Cybercrimes Classification (Co...
43
Cybercrimes Classification (Contd.)
44
Cybercrimes Classification (Contd.)
Cybercrimes Classification (Contd.)
• Against Individual
– Spamming: Spamming 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.
Unit 1
Nishant Doshi
Click to add notes

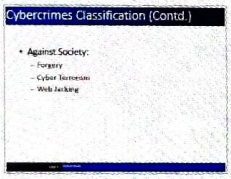

Cybercrimes Classification (Contd.)
• Against property:
– Credit card frauds: Credit card fraud is the unauthorized use of a credit or debit card, or similar payment tool (ACH, EFT, recurring charge, etc.), to fraudulently obtain money or property.
Unit 1 Nishant Doshi
42 Cybercrimes Classification (Contd.)
43 Cybercrimes Classification (Contd.)
44 Cybercrimes Classification (Contd.)
45 Cybercrimes Classification (Contd.)
Click to add notes

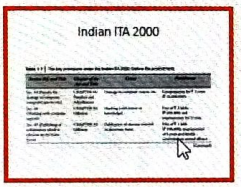

Unit 1.pptx - PowerPoint
FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Aashka R
Cut
Copy
Format Painter
Paste
New Slide
Layout
Reset
Section
Clipboard
Slides
Font
Text Direction
Align Text
Convert to SmartArt
Paragraph
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Drawing
Find
Replace
Select
Editing
43 Cybercrimes Classification (Contd.)
44 Cybercrimes Classification (Contd.)
45 Cybercrimes Classification (Contd.)
46 Cybercrimes Classification (Contd.)
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.
Unit 1
Nishant Doshi
Click to add notes

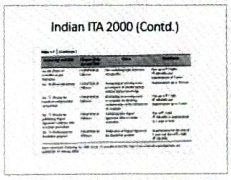

Unit 1.pptx - PowerPoint
Aashka R
FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Cut
Copy
Format Painter
Paste
Layout
Reset
Section
New Slide
Clipboard
Slides
Font
Text Direction
Align Text
Convert to SmartArt
Paragraph
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Drawing
Find
Replace
Select
Editing
44
Cybercrimes Classification (Contd.)
45
Cybercrimes Classification (Contd.)
46
Cybercrimes Classification (Contd.)
47
Indian ITA 2000
Cybercrimes Classification (Contd.)
Against Organization:
– Unauthorized accessing of computer
– Virus Attacks
– E-Mail bombing
– Trojan Horse
– Software piracy
Unit 1
Nishant Doshi
Click to add notes

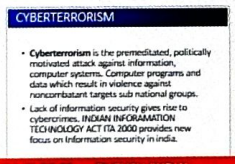

Unit 1.pptx - PowerPoint
Aashka R
FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Cut
Copy
Format Painter
Paste
New Slide
Layout
Reset
Section
Clipboard
Slides
Font
Text Direction
Align Text
Convert to SmartArt
Paragraph
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Drawing
Find
Replace
Select
Editing
45
Cybercrimes Classification (Contd.)
46
Cybercrimes Classification (Contd.)
Cybercrimes Classification (Co...
47
Indian ITA 2000
48
Indian ITA 2000 (Contd.)
Cybercrimes Classification (Contd.)
• Against Society:
– Forgery
– Cyber Terrorism
– Web Jacking
Unit 1
Nishant Doshi
Click to add notes



46


47


48


49 *


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)

Click to add notes

Unit 1.pptx - PowerPoint

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Aashka R.

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

47 Indian ITA 2000

48 Indian ITA 2000 (Contd.)

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 INFORAMATION 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.

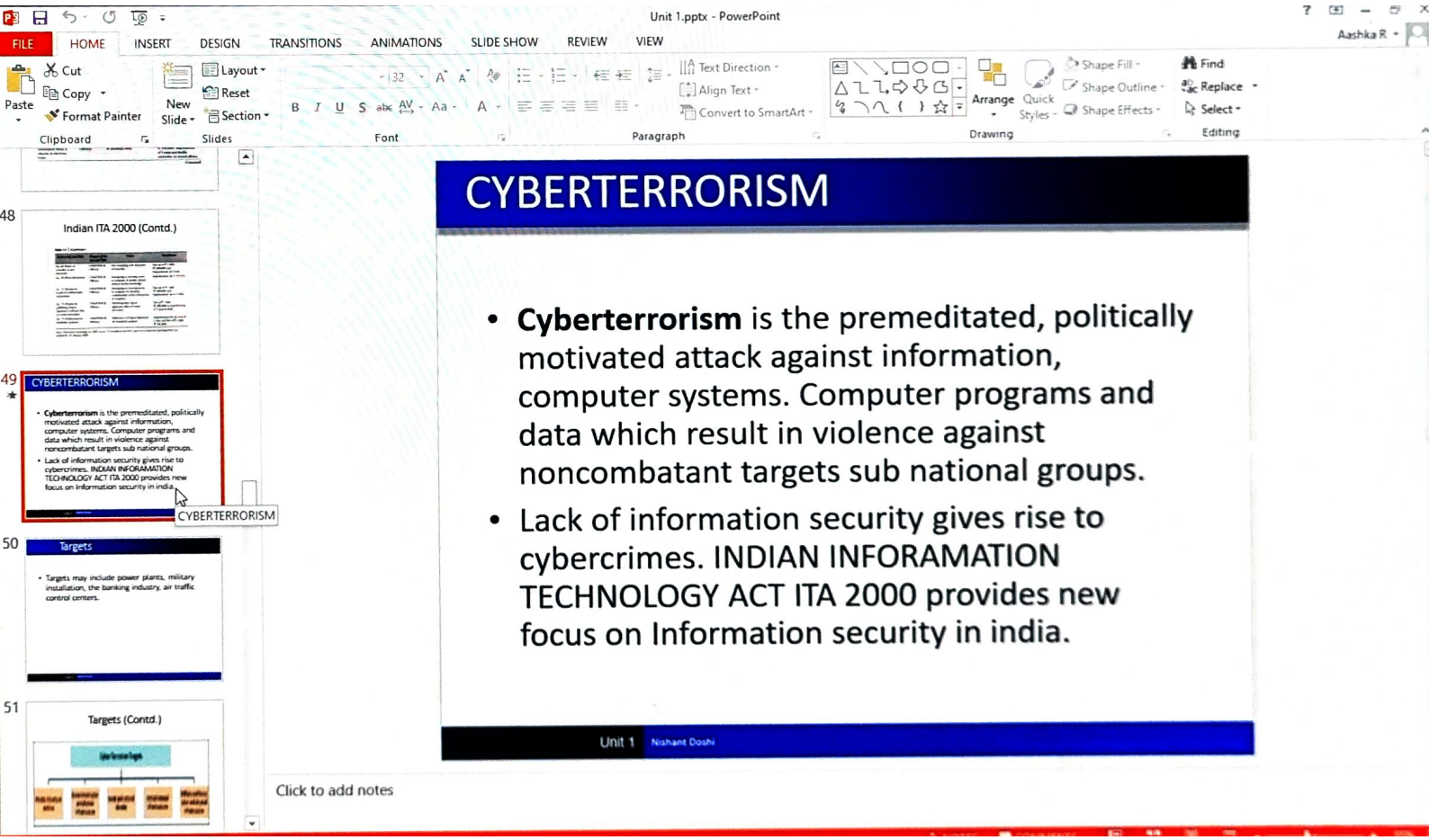
Indian ITA 2000 (Contd.)

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/ (22 February 2000).

Click to add notes


Unit 1.pptx - PowerPoint
FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Aashka R.
Cut
Copy
Format Painter
Paste
Clipboard
New Slide
Layout
Reset
Section
Slides
Font
Text Direction
Align Text
Convert to SmartArt
Paragraph
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Drawing
Find
Replace
Select
Editing
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 INFORAMATION TECHNOLOGY ACT ITA 2000 provides new focus on information security in india.
CYBERTERRORISM
50
Targets
Targets may include power plants, military installation, the banking industry, air traffic control centers.
51
Targets (Contd.)
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 INFORAMATION TECHNOLOGY ACT ITA 2000 provides new focus on Information security in india.
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 Layout Reset Section New Slide Clipboard Slides Font Paragraph Text Direction Align Text Convert to SmartArt Arrange Quick Styles Shape Fill Shape Outline Shape Effects Drawing Find Replace Select Editing

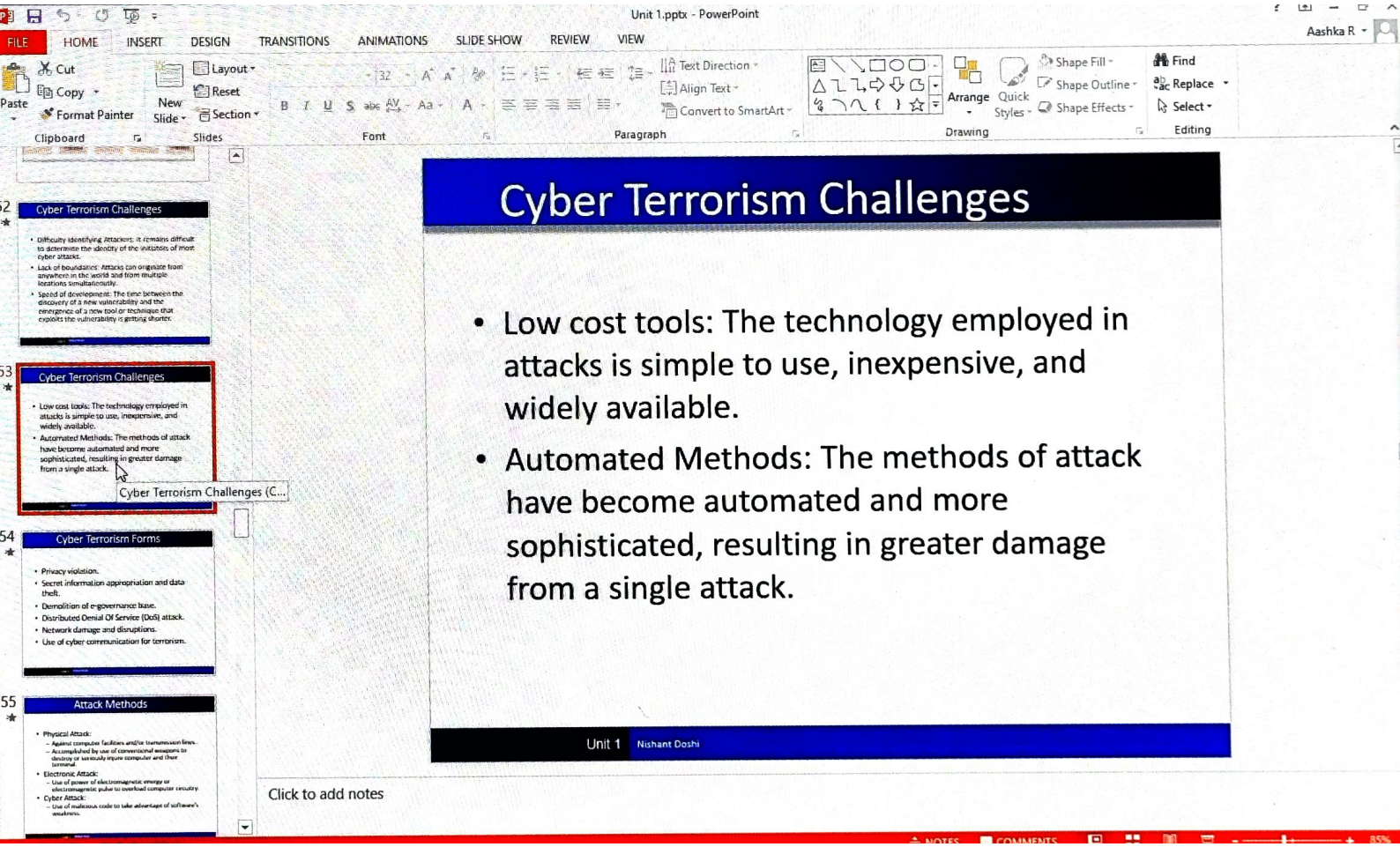
Targets

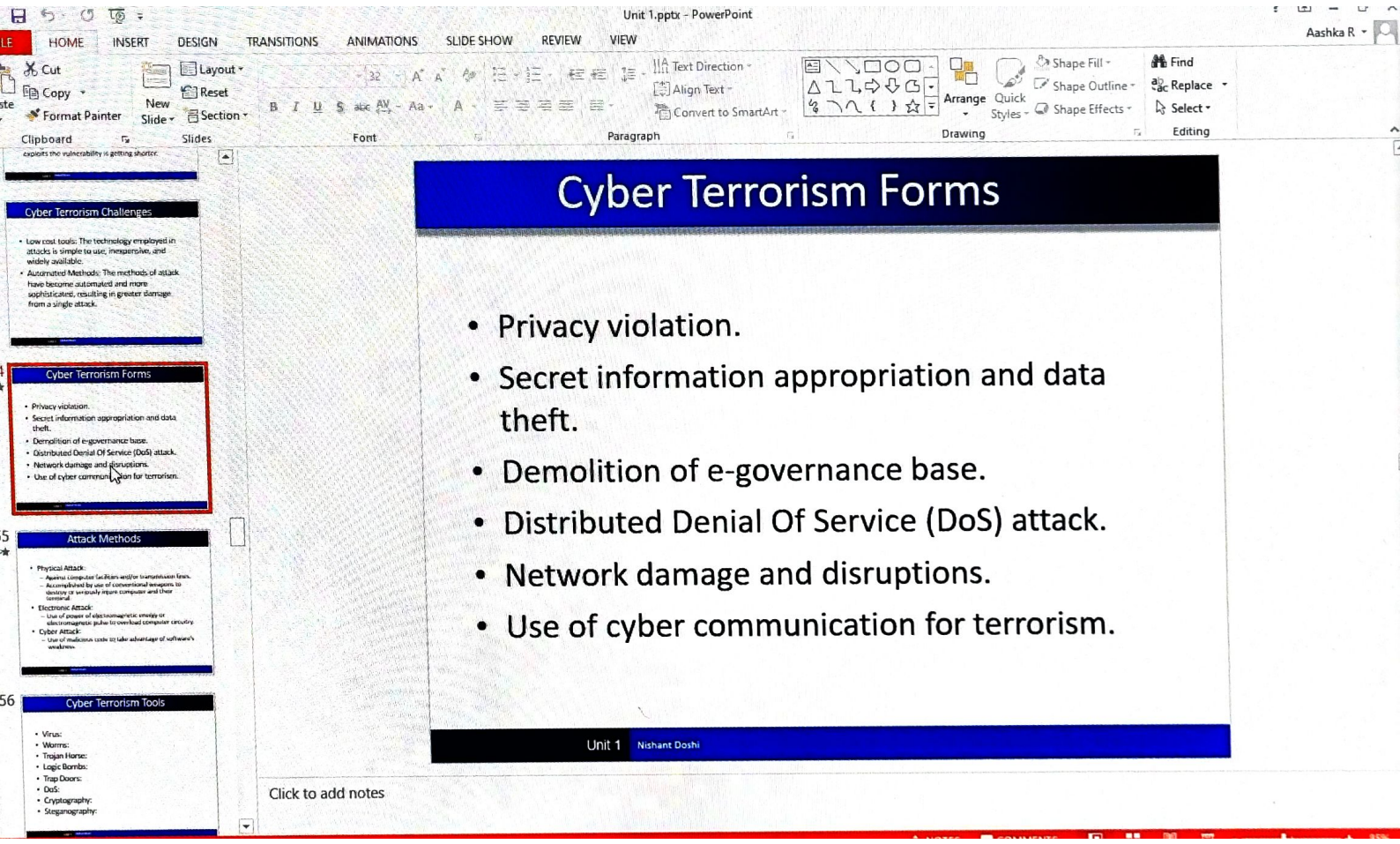
- Targets may include power plants, military installation, the banking industry, air traffic control centers.

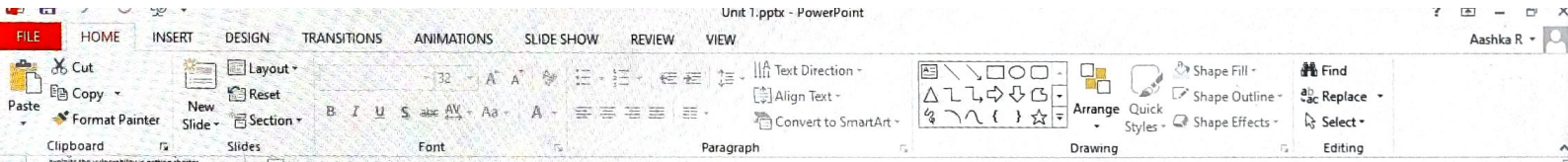
Click to add notes

FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Aashka R
Paste
Cut
Copy
Format Painter
New Slide
Layout
Reset
Section
Text Direction
Align Text
Convert to SmartArt
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Find
Replace
Select
Clipboard
Slides
Font
Paragraph
Drawing
Editing
• Targets may include power plants, military installation, the banking industry, air traffic control centers.
51
Targets (Contd.)
Targets (Contd.)
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
Targets (Contd.)
Cyber Terrorism Tragets
Private industry or entities
Government cyber and physical infrastructure
Social and national identity
Critical national infrastructures
Military and forces cyber and physical infrastructure
Click to add notes
NOTES
COMMENTS
85%

Unit 1.pptx - PowerPoint
FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Aashka R
Cut
Copy
Format Painter
Paste
Layout
Reset
Section
New Slide
Clipboard
Slides
Font
Text Direction
Align Text
Convert to SmartArt
Paragraph
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Drawing
Find
Replace
Select
Editing
• Targets may include power plants, military installation, the banking industry, air traffic control centers.
51
Targets (Contd.)
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
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.
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
Layout
Reset
Section
Clipboard
Slides
Font
Text Direction
Align Text
Convert to SmartArt
Paragraph
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Drawing
Find
Replace
Select
Editing
52
Cyber Terrorism Challenges
53
Cyber Terrorism Challenges
Cyber Terrorism Challenges (C...
54
Cyber Terrorism Forms
55
Attack Methods
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.
Unit 1
Nishant Doshi
Click to add notes


Unit 1.pptx - PowerPoint
Aashka R
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Cut
Copy
Format Painter
New Slide
Layout
Reset
Section
Text Direction
Align Text
Convert to SmartArt
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Find
Replace
Select
Clipboard
Slides
Font
Paragraph
Drawing
Editing
Cyber Terrorism Challenges
Cyber Terrorism Forms
Attack Methods
Cyber Terrorism Tools
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.
Unit 1
Nishant Doshi
Click to add notes



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.
• Demolition of e-governance base.
• Distributed Denial Of Service (DoS) attack.
• Network damage and disruptions.
• Use of cyber communication for terrorism.

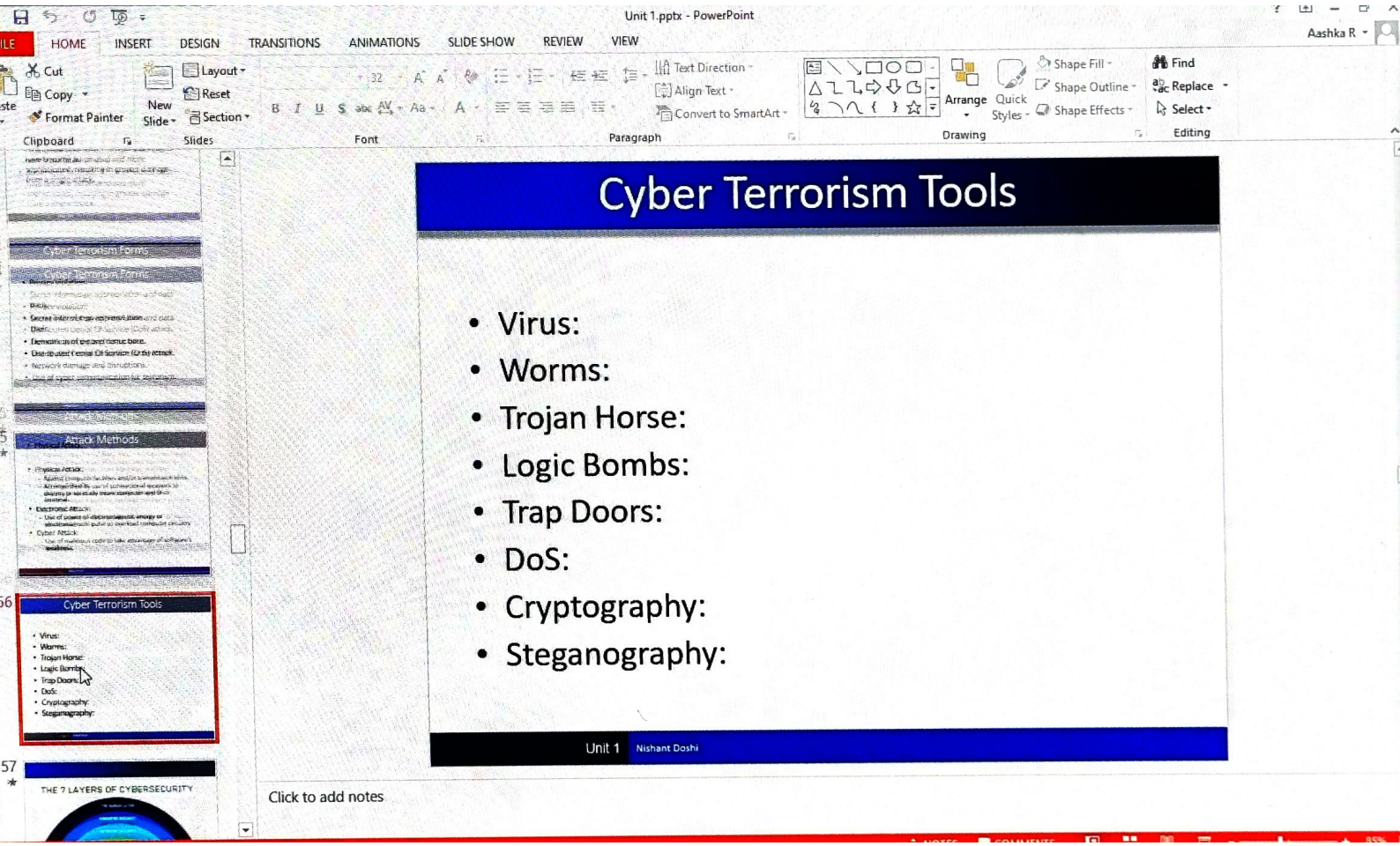
55
Attack Methods
• Physical Attack:
– Against computer facilities and/or transmission lines.
– Accomplished by use of conventional weapons to destroy or seriously injure computer and their terminal.
• Electronic Attack:
– Use of power of electromagnetic energy or electromagnetic pulse to overload computer 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:

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.

Click to add notes


Unit 1.pptx - PowerPoint
Aashka R
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Cut
Copy
Format Painter
New Slide
Layout
Reset
Section
Text Direction
Align Text
Convert to SmartArt
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Find
Replace
Select
Clipboard
Slides
Font
Paragraph
Drawing
Editing
Cyber Terrorism Tools
Virus:
Worms:
Trojan Horse:
Logic Bombs:
Trap Doors:
DoS:
Cryptography:
Steganography:
Unit 1
Nishant Doshi
Click to add notes

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Paste Cut Copy Format Painter | New Slide Layout Reset Section | Clipboard Slides | Font | Paragraph | Text Direction Align Text Convert to SmartArt | Drawing | Arrange Quick Styles Shape Fill Shape Outline Shape Effects | Editing Find Replace Select

56

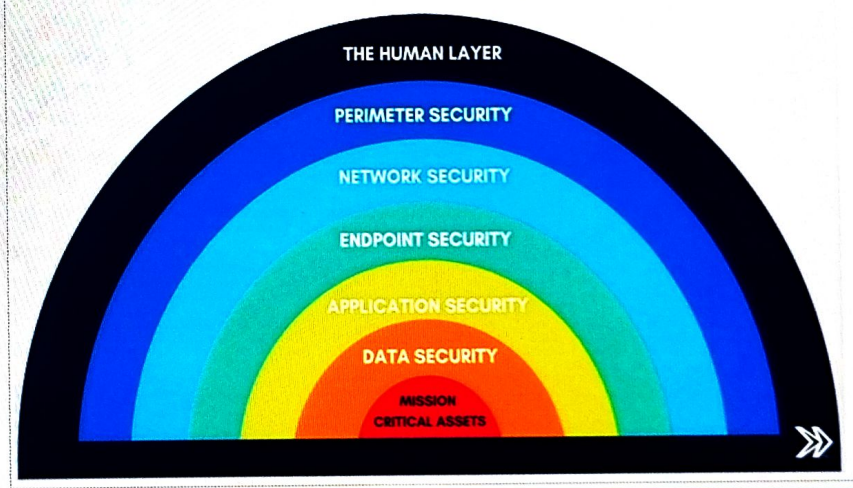
57

58

59

Click to add title

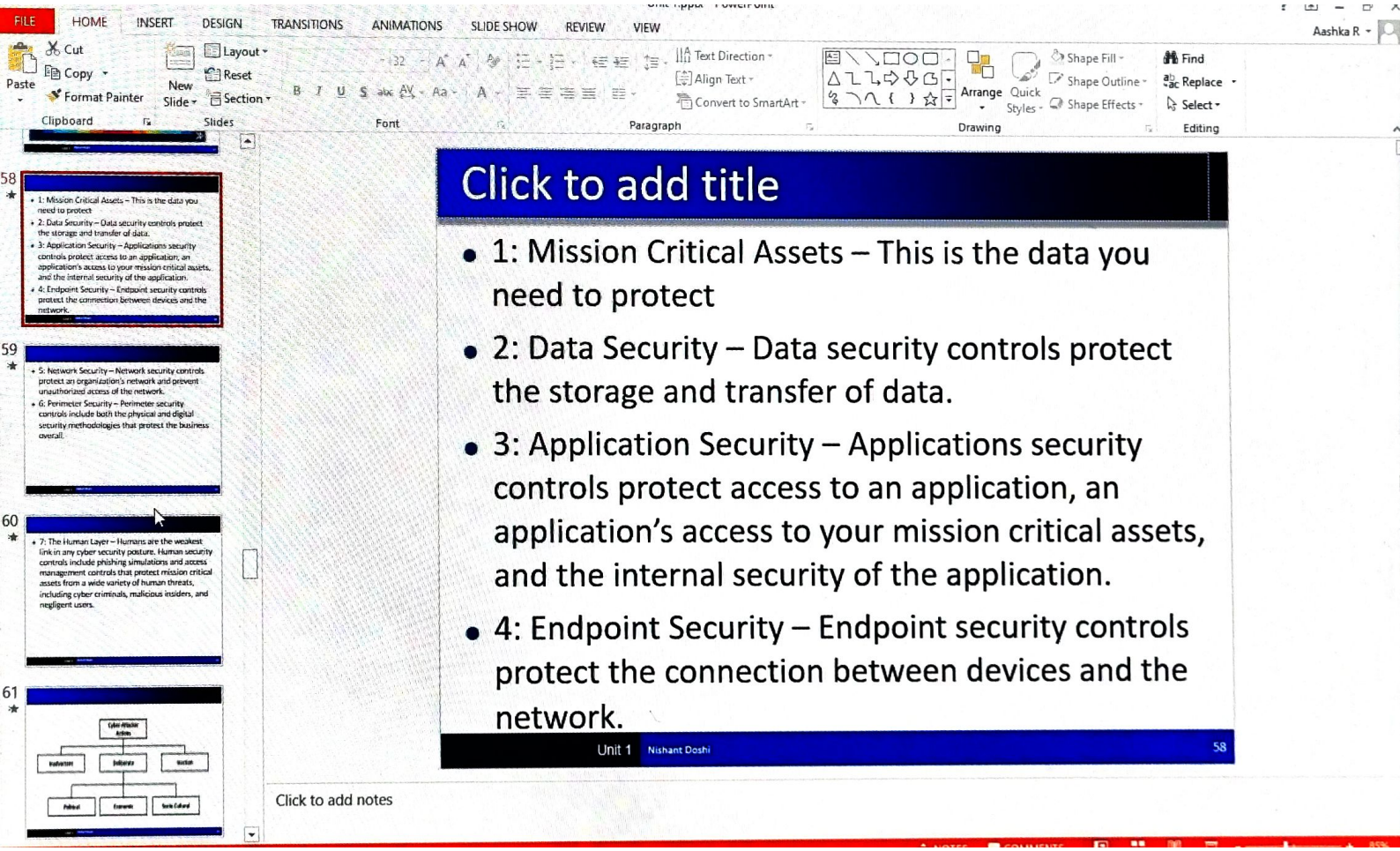
THE 7 LAYERS OF CYBERSECURITY

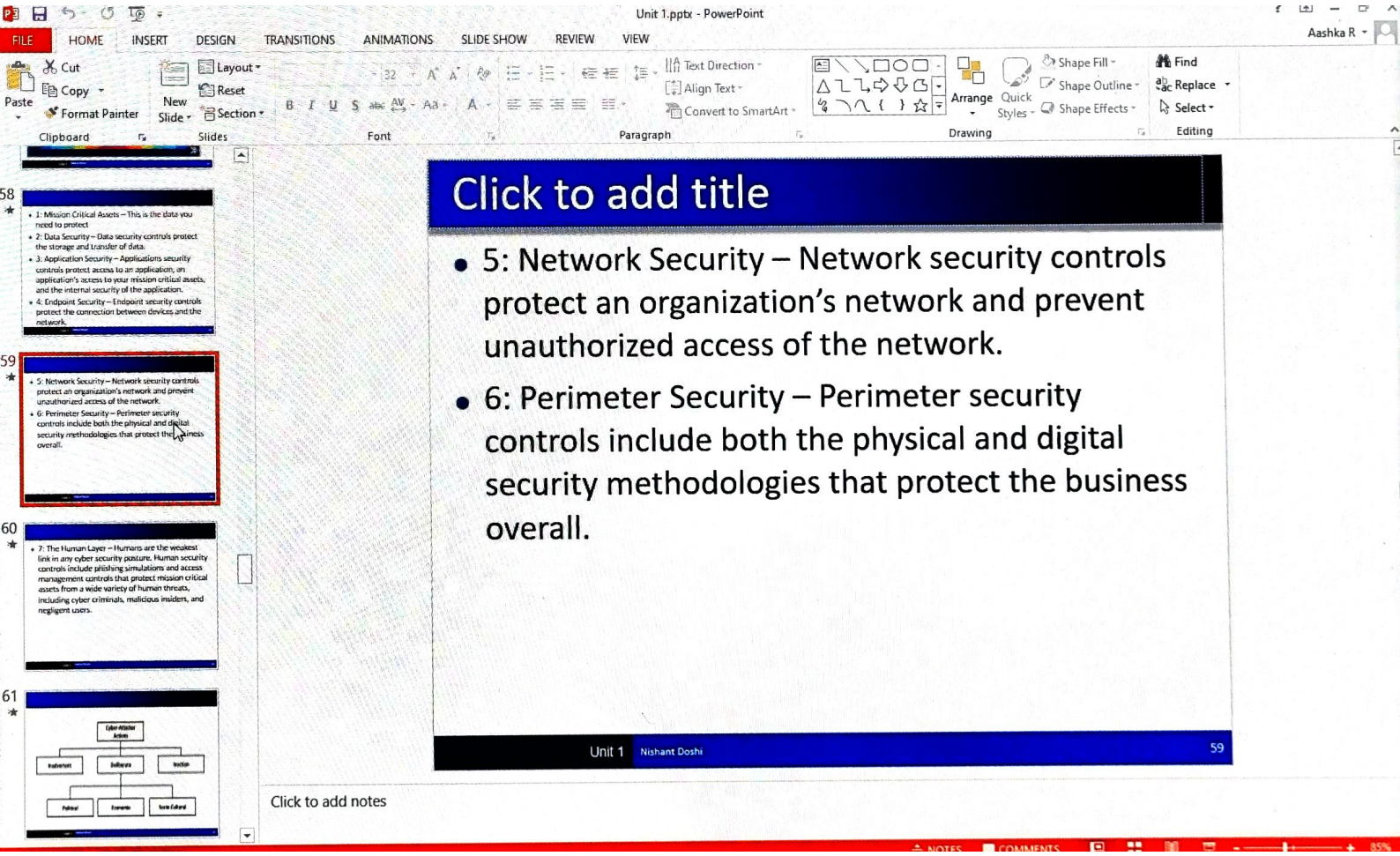


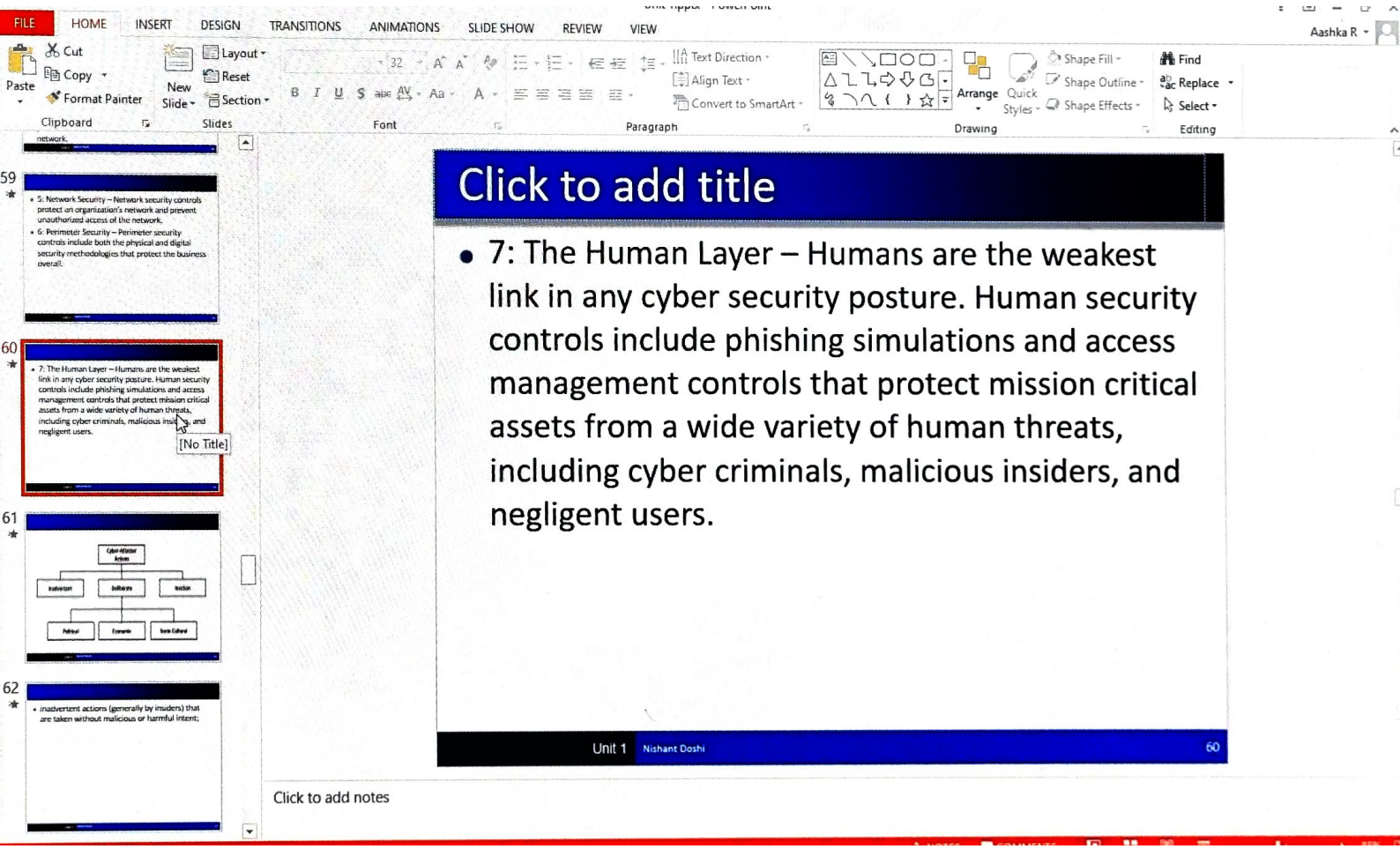
Unit 1 Nishant Doshi 57

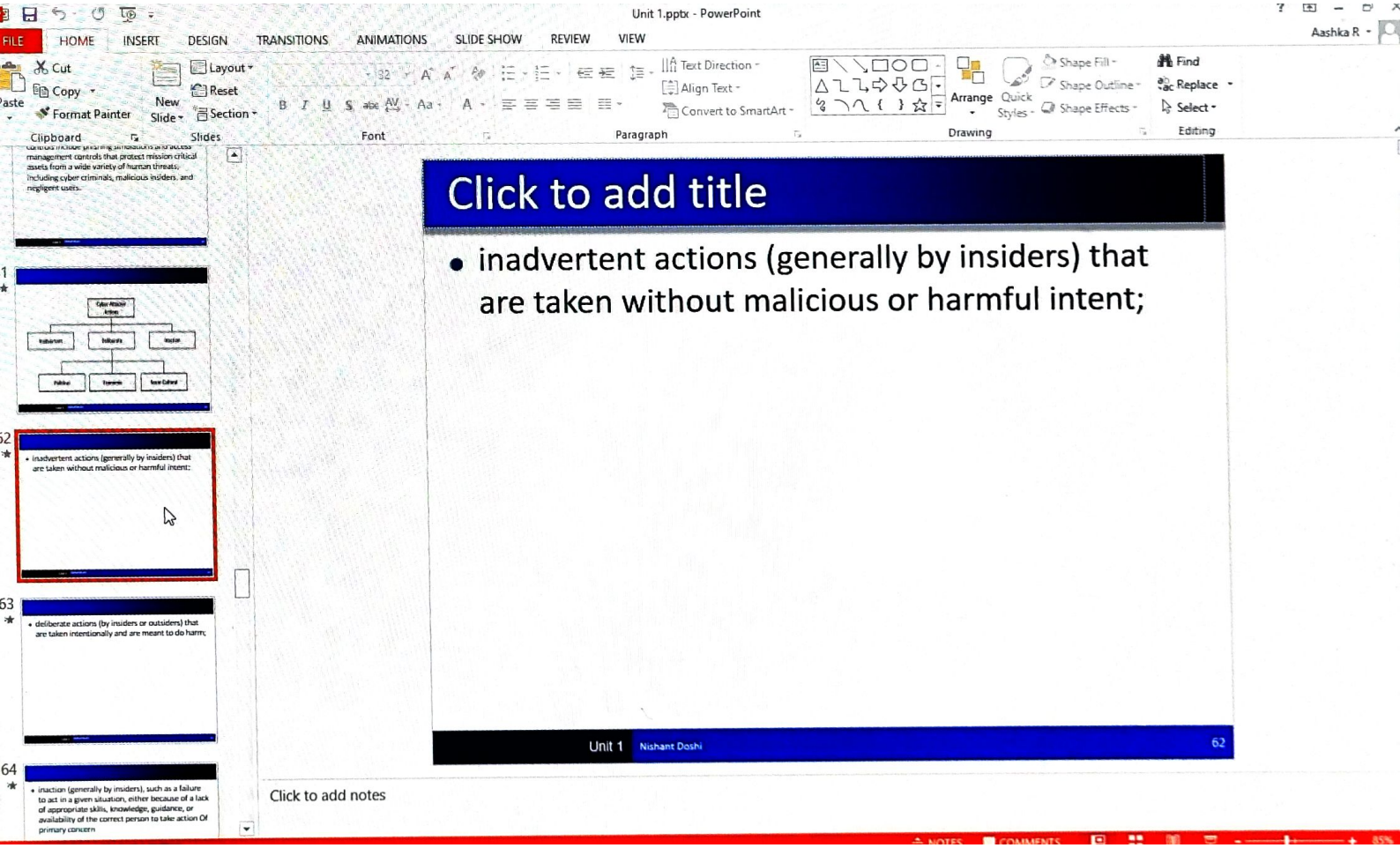
Click to add notes

NOTES COMMENTS


FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Aashka R
Cut
Copy
Format Painter
Paste
Layout
Reset
Section
New Slide
Clipboard
Slides
Font
Text Direction
Align Text
Convert to SmartArt
Paragraph
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Drawing
Find
Replace
Select
Editing
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 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.
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.
Unit 1
Nishant Doshi
58
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
Layout
Reset
Section
Text Direction
Align Text
Convert to SmartArt
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Find
Replace
Select
Clipboard
Slides
Font
Paragraph
Drawing
Editing
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 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.
61
Click to add title
• 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.
Unit 1
Nishant Doshi
59
Click to add notes
NOTES
COMMENTS
85%


FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Aashka R
Cut
Copy
Format Painter
Paste
New Slide
Layout
Reset
Section
Clipboard
Slides
Font
Text Direction
Align Text
Convert to SmartArt
Paragraph
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Drawing
Find
Replace
Select
Editing
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 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
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.
Unit 1
Nishant Doshi
60
Click to add notes


Unit 1.pptx - PowerPoint
FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Aashka R
Cut
Copy
Format Painter
Paste
New Slide
Layout
Reset
Section
Clipboard
Slides
Font
Text Direction
Align Text
Convert to SmartArt
Paragraph
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Drawing
Find
Replace
Select
Editing
Click to add title
• inadvertent actions (generally by insiders) that are taken without malicious or harmful intent;
Unit 1
Nishant Doshi
62
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 Layout Reset 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

62
- 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

[No Title]

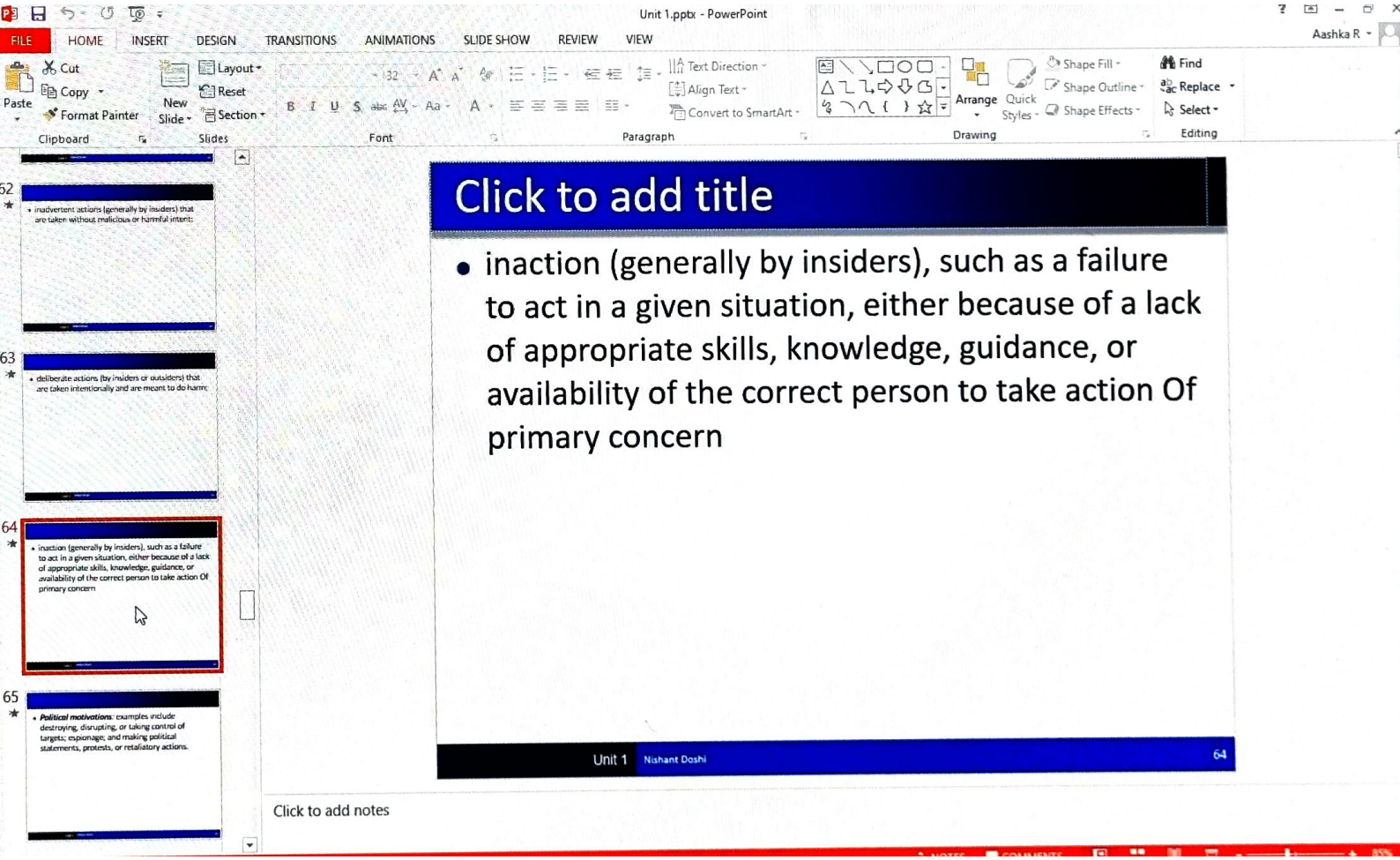
65
- **Political motivations**: examples include destroying, disrupting, or taking control of targets; espionage; and making political statements, protests, or retaliatory actions.

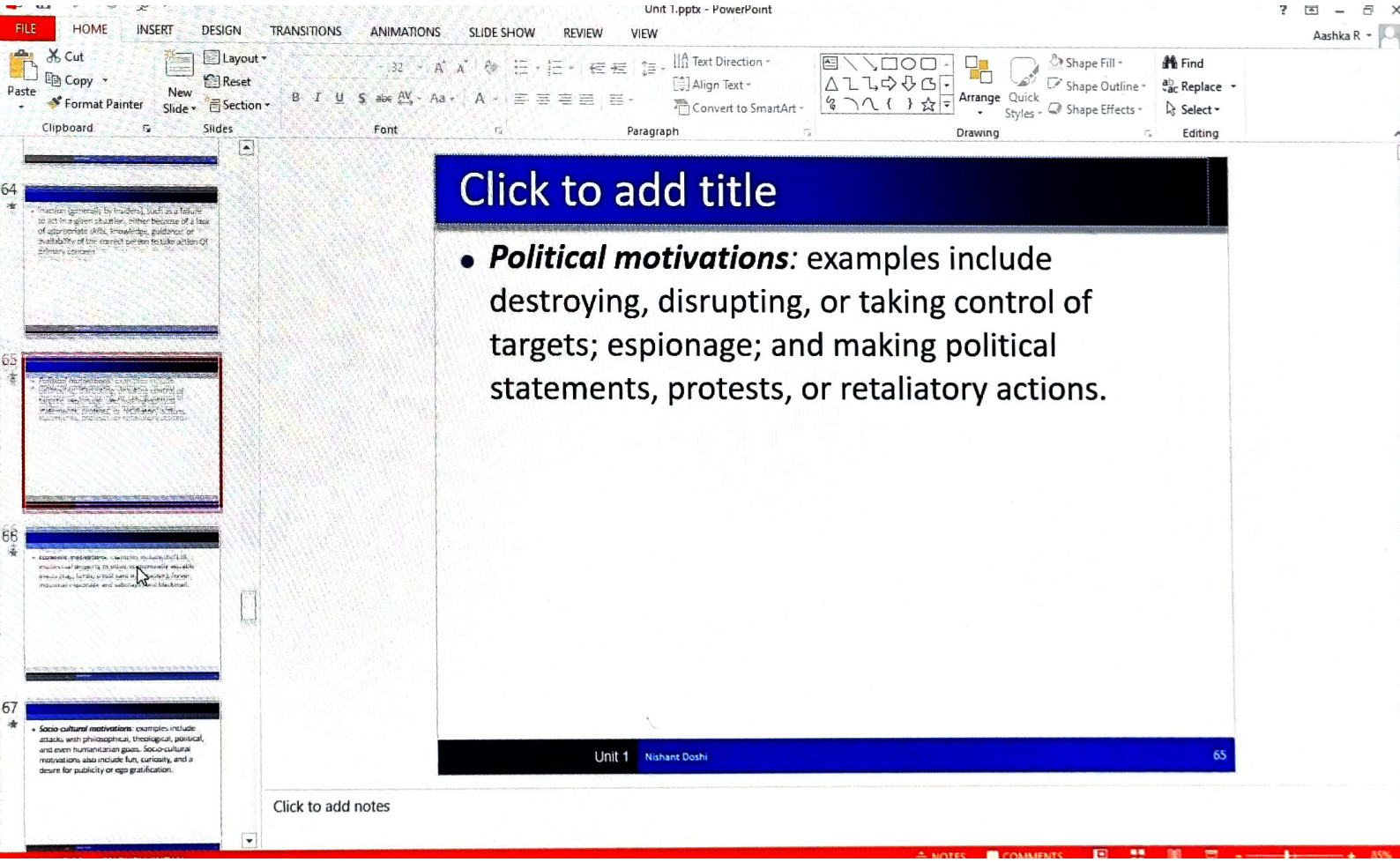
Click to add title

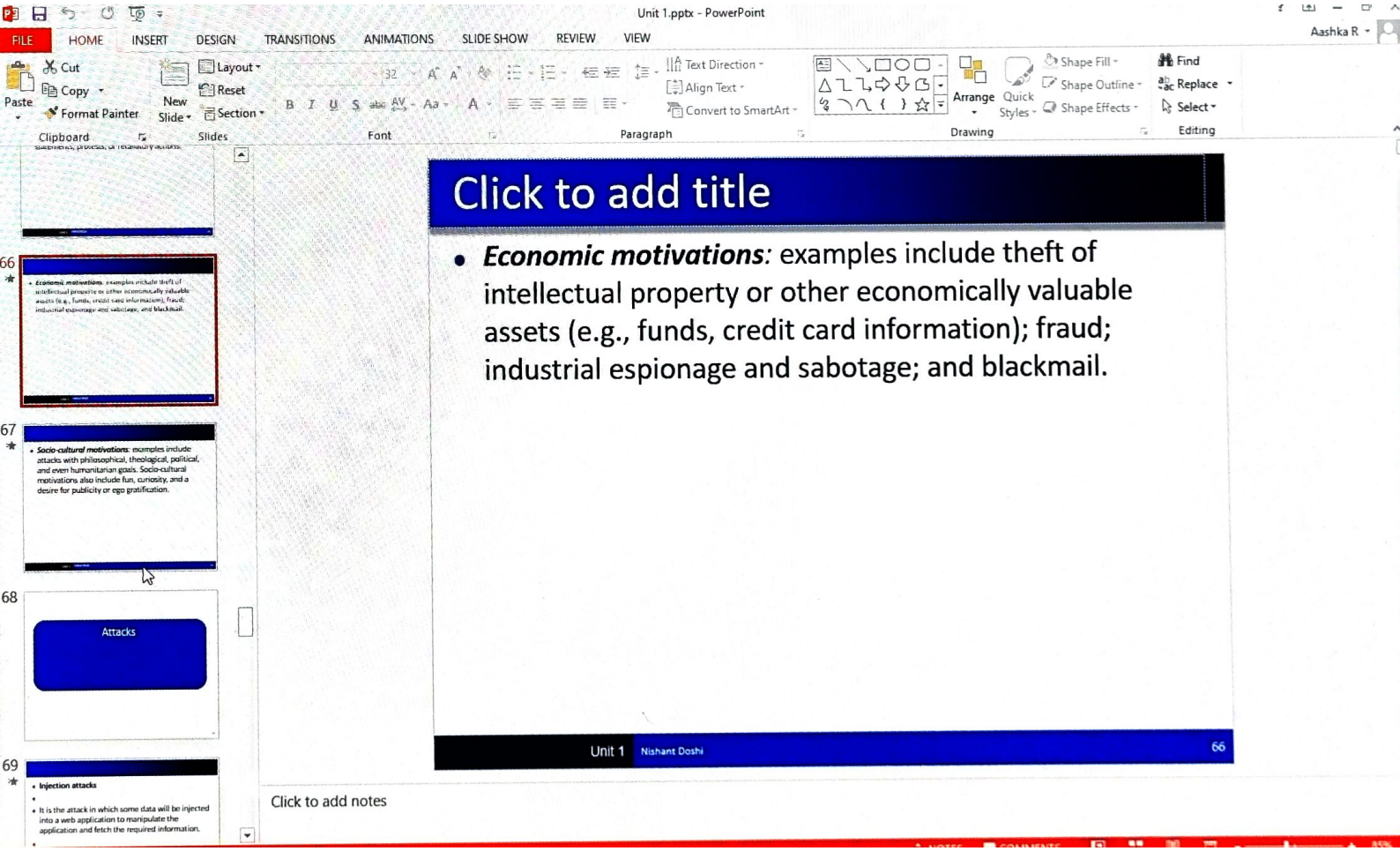
- deliberate actions (by insiders or outsiders) that are taken intentionally and are meant to do harm;

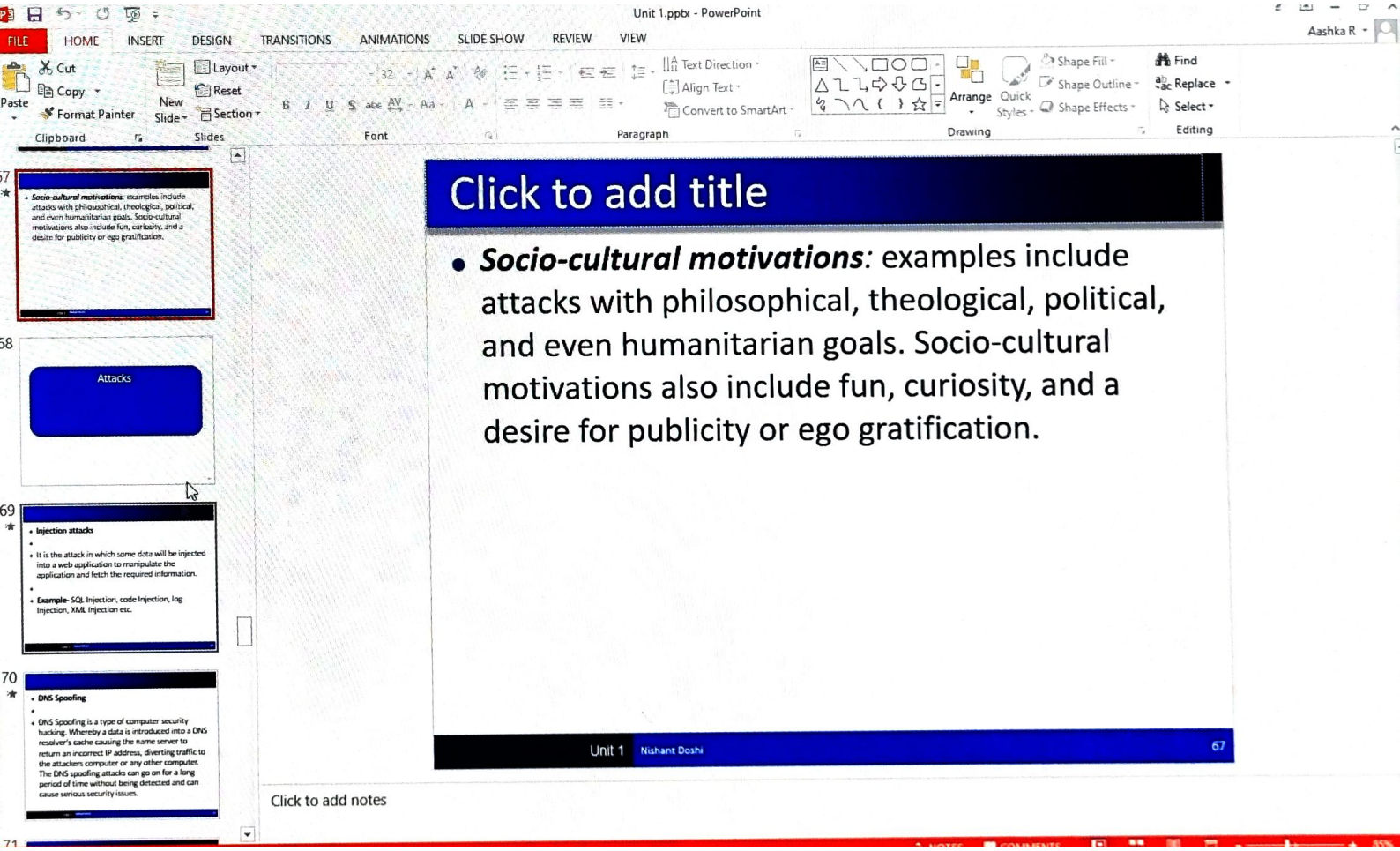
Unit 1 Nishant Doshi 63

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
Clipboard
New Slide
Layout
Reset
Section
Slides
Text Direction
Align Text
Convert to SmartArt
Paragraph
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Drawing
Find
Replace
Select
Editing
62
• 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
Unit 1
Nishant Doshi
64
Click to add notes


Unit 1.pptx - PowerPoint
FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Aashka R
Paste
Cut
Copy
Format Painter
New Slide
Layout
Reset
Section
Text Direction
Align Text
Convert to SmartArt
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Find
Replace
Select
Clipboard
Slides
Font
Paragraph
Drawing
Editing
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.
Unit 1
Nishant Doshi
65
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
Clipboard
Layout
Reset
Section
New Slide
Slides
Font
Text Direction
Align Text
Convert to SmartArt
Paragraph
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Drawing
Find
Replace
Select
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, 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.
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.
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
Paste
Layout
Reset
New Slide
Section
Clipboard
Slides
Font
Text Direction
Align Text
Convert to SmartArt
Paragraph
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Drawing
Find
Replace
Select
Editing
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 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
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.
Unit 1
Nishant Doshi
67
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 Layout Reset Section | Clipboard Slides | Font | Text Direction Align Text Convert to SmartArt | Paragraph | Arrange Quick Styles Shape Fill Shape Outline Shape Effects | Drawing | Find Replace Select | Editing

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 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.

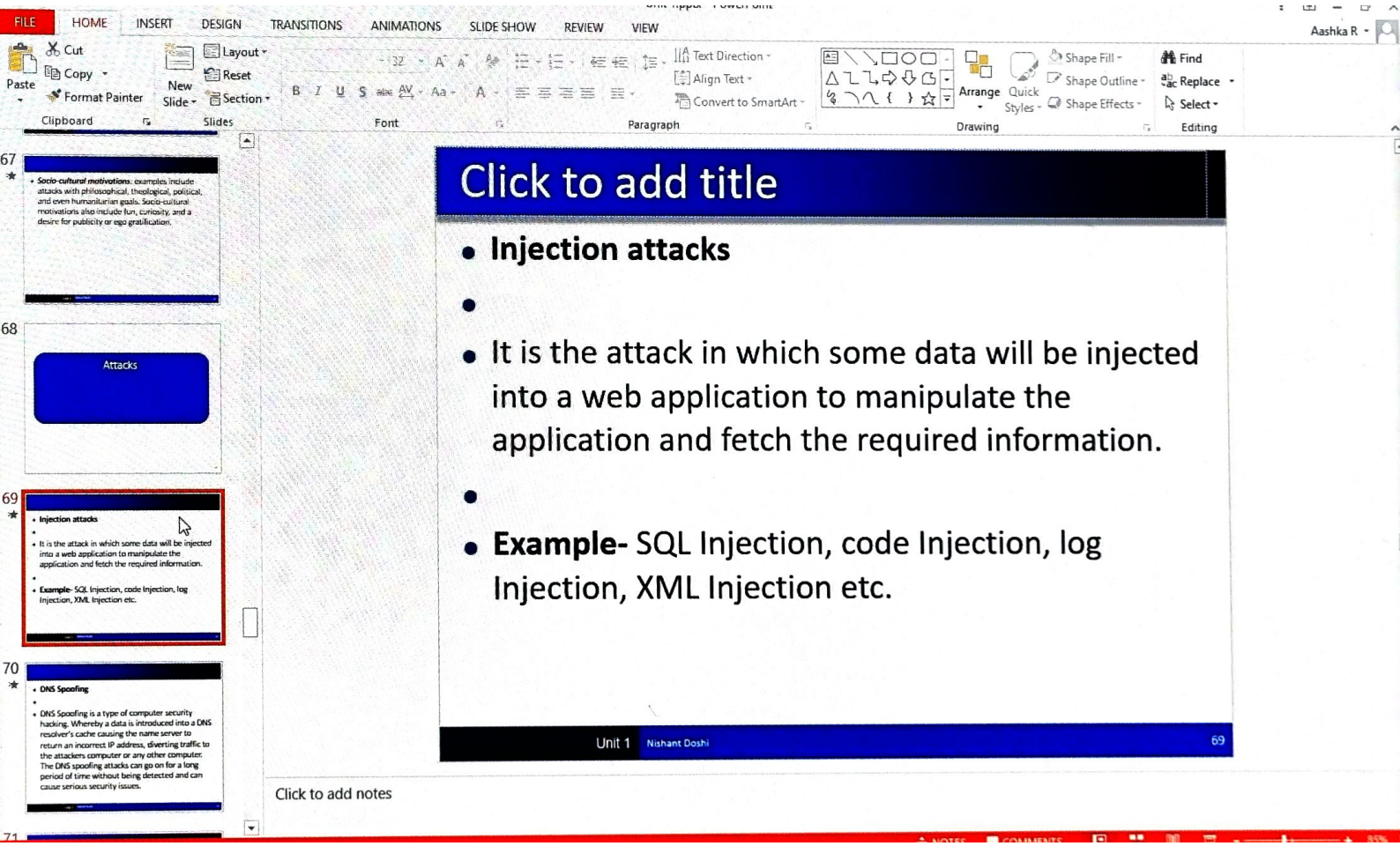
71

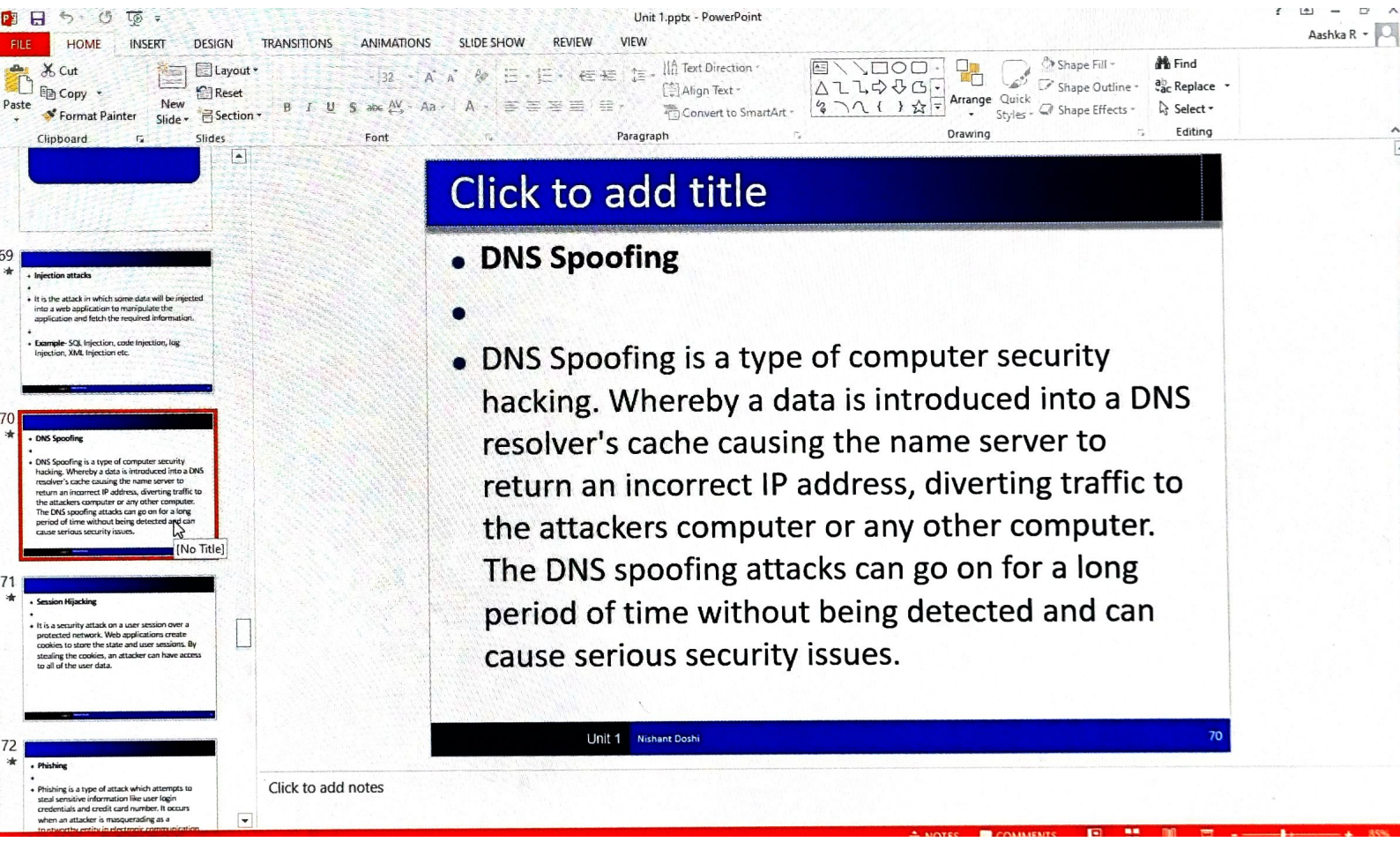
Attacks

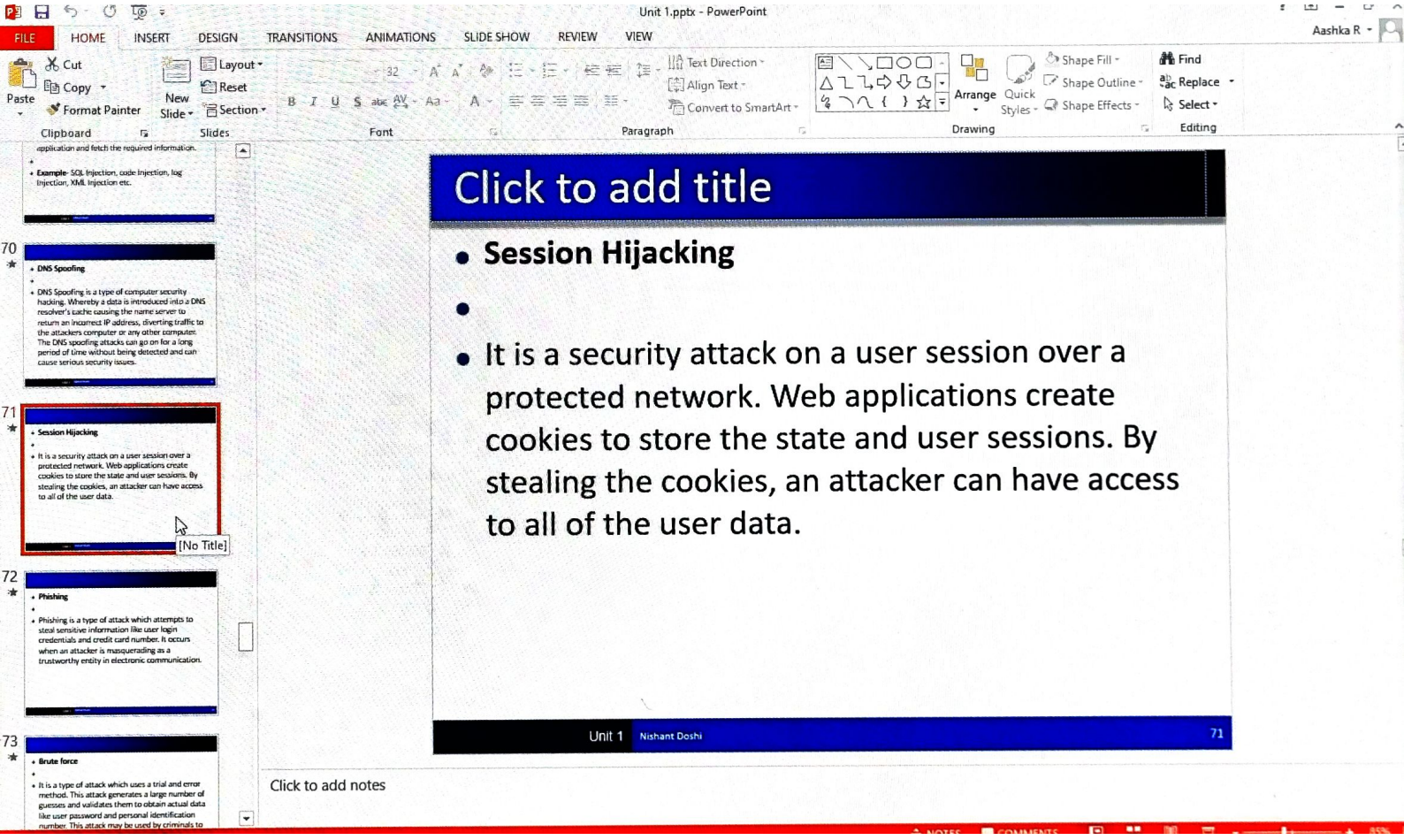
Click to add subtitle

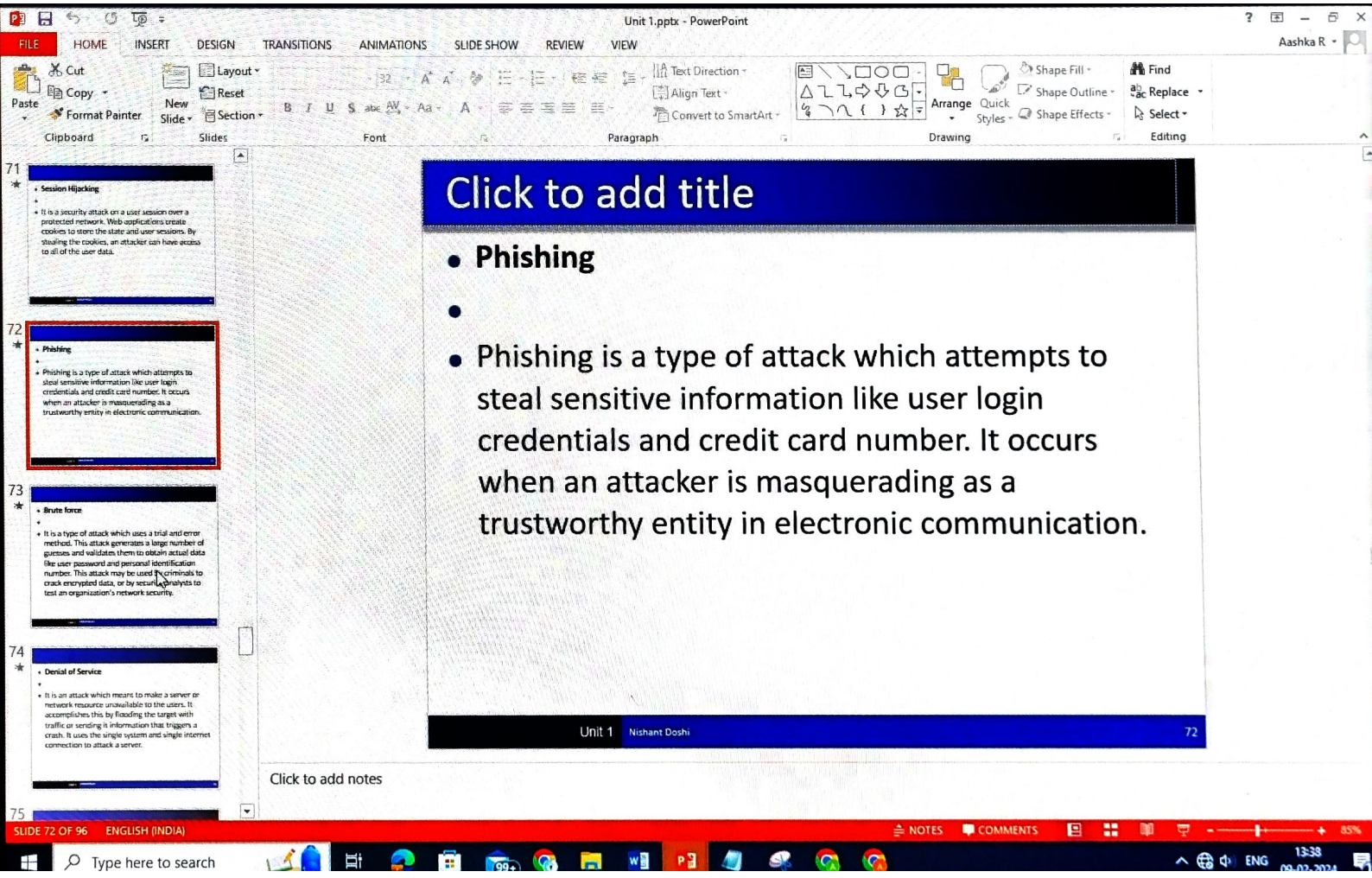
68

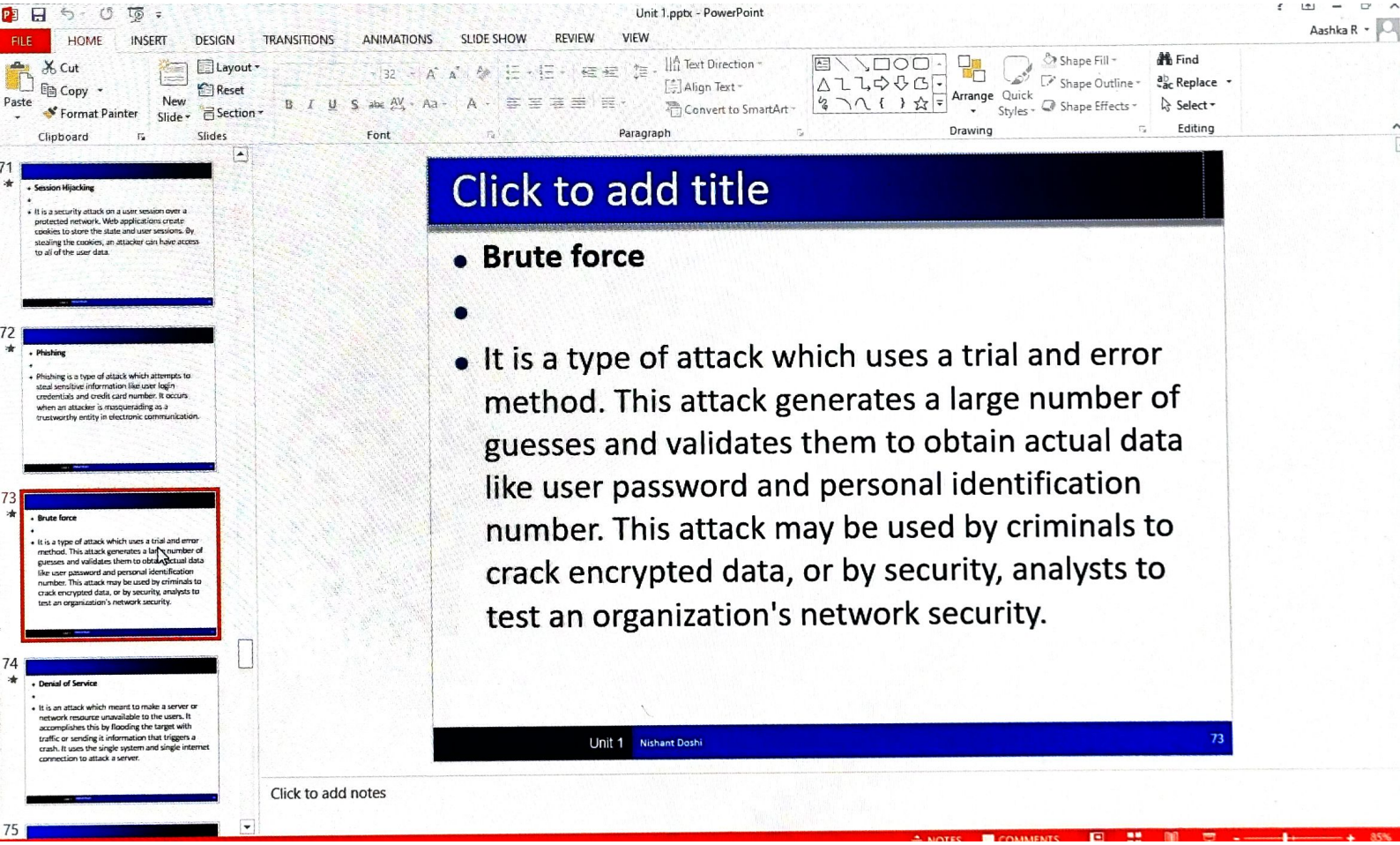
Click to add notes

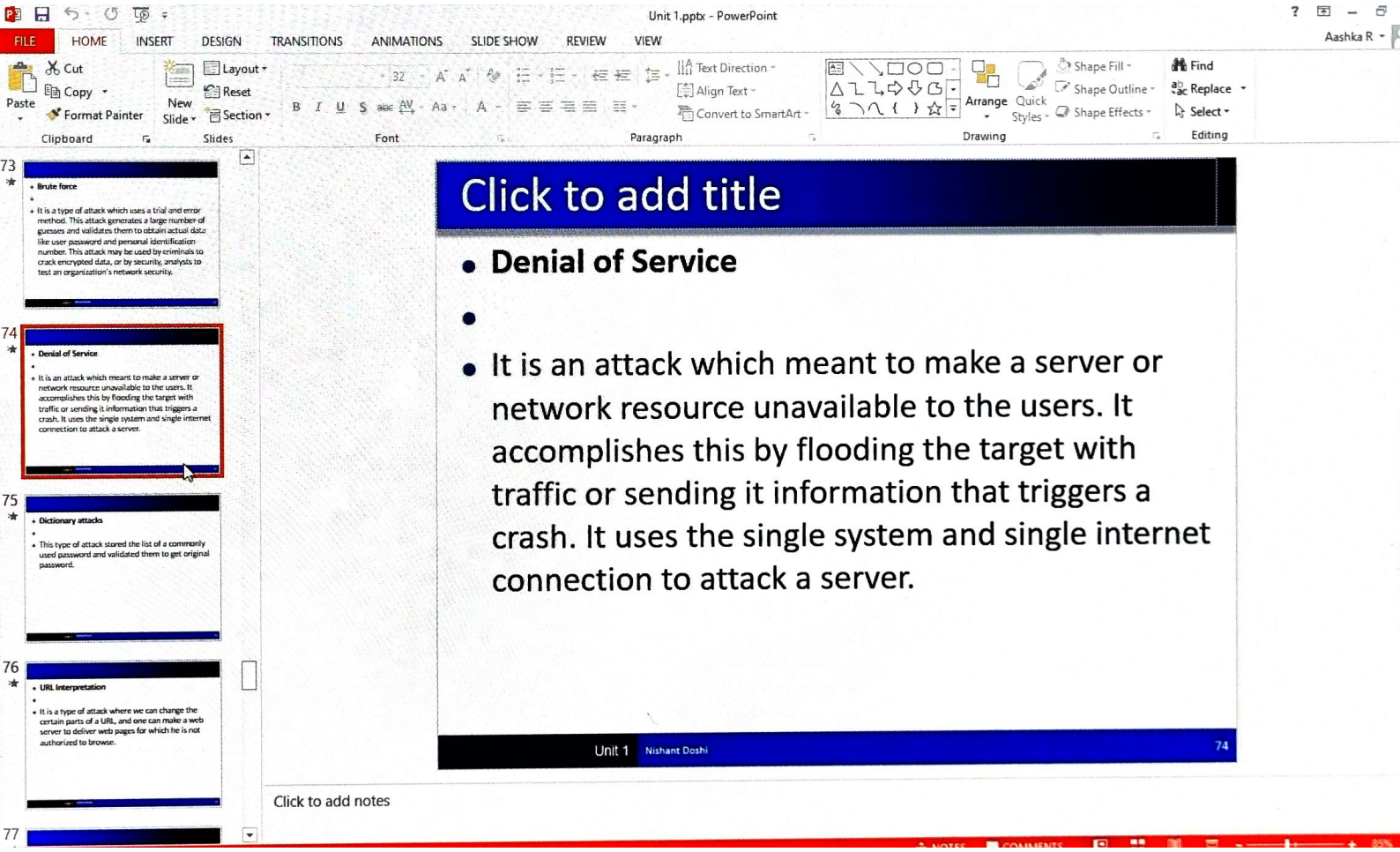

FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Aashka R
Cut
Copy
Format Painter
Paste
Layout
Reset
New Slide
Section
Clipboard
Slides
Font
Text Direction
Align Text
Convert to SmartArt
Paragraph
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Drawing
Find
Replace
Select
Editing
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 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.
Click to add title
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.
Unit 1
Nishant Doshi
69
Click to add notes

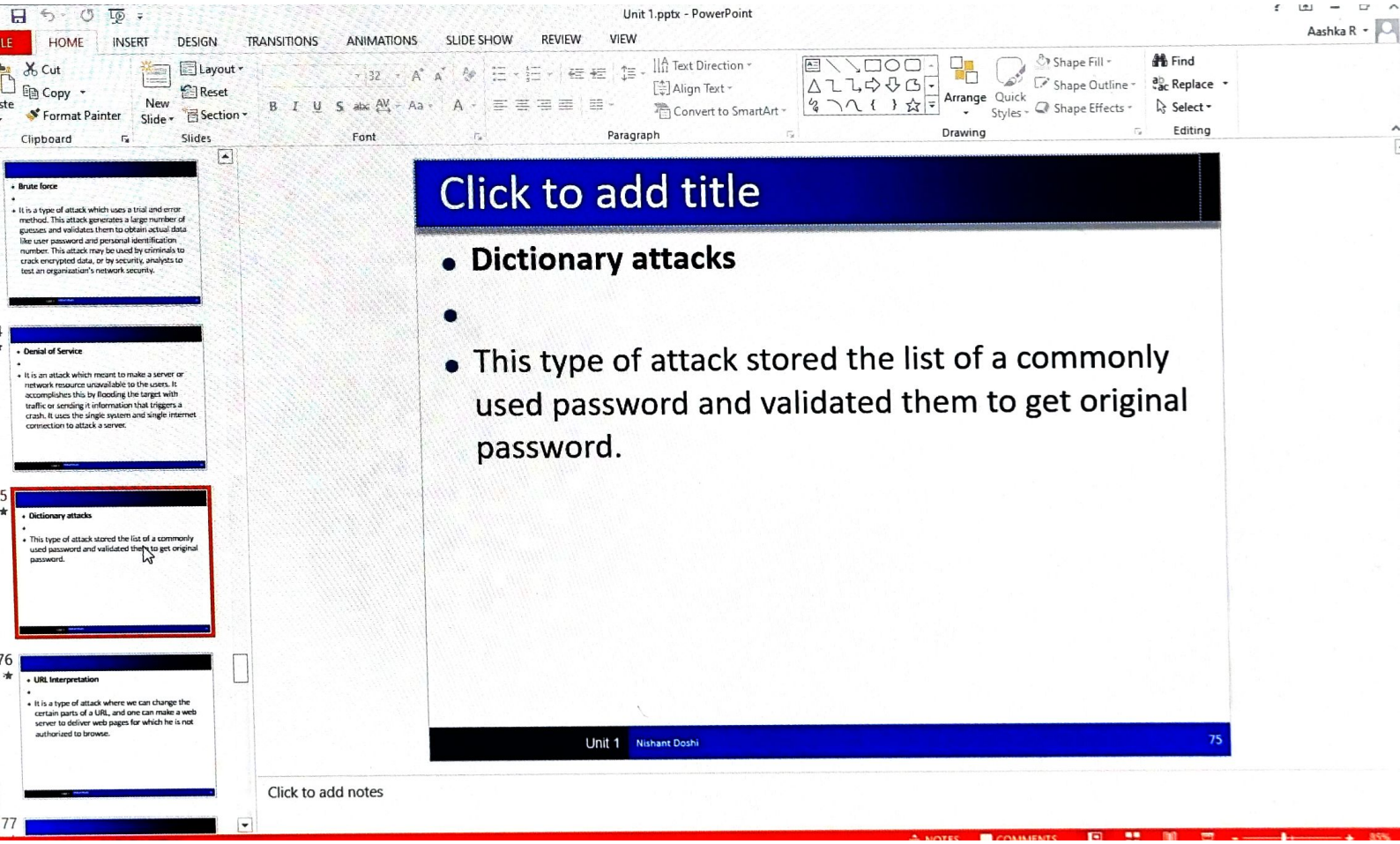

Unit 1.pptx - PowerPoint
FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Aashka R
Cut
Copy
Format Painter
Paste
New Slide
Layout
Reset
Section
Clipboard
Slides
Font
Text Direction
Align Text
Convert to SmartArt
Paragraph
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Drawing
Find
Replace
Select
Editing
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 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.
[No Title]
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
Click to add title
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.
Unit 1
Nishant Doshi
70
Click to add notes

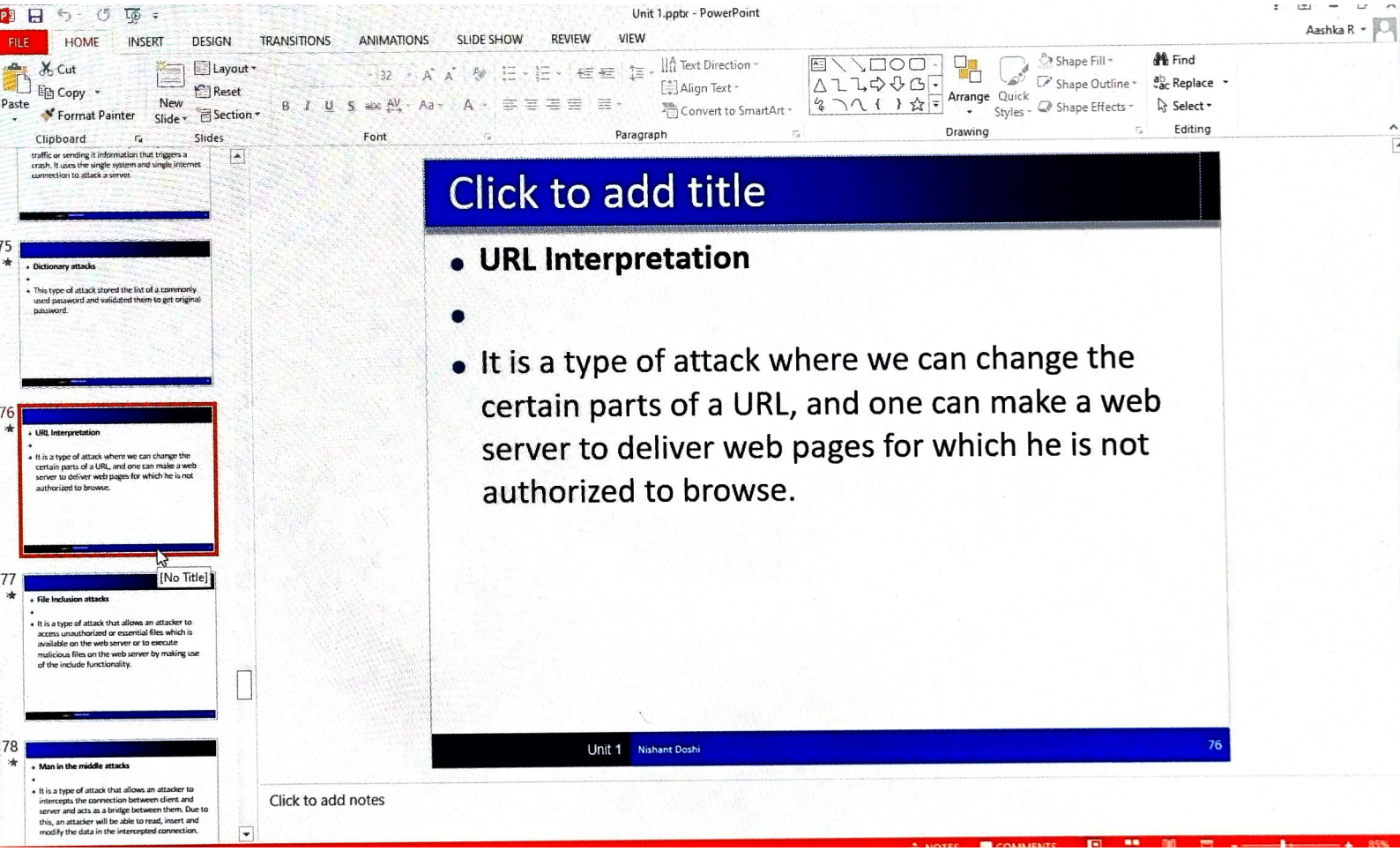

Unit 1.pptx - PowerPoint
Aashka R
FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Cut
Copy
Format Painter
Paste
Layout
Reset
Section
New Slide
Clipboard
Slides
Font
Text Direction
Align Text
Convert to SmartArt
Paragraph
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Drawing
Find
Replace
Select
Editing
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 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.
Unit 1
Nishant Doshi
71
Click to add notes

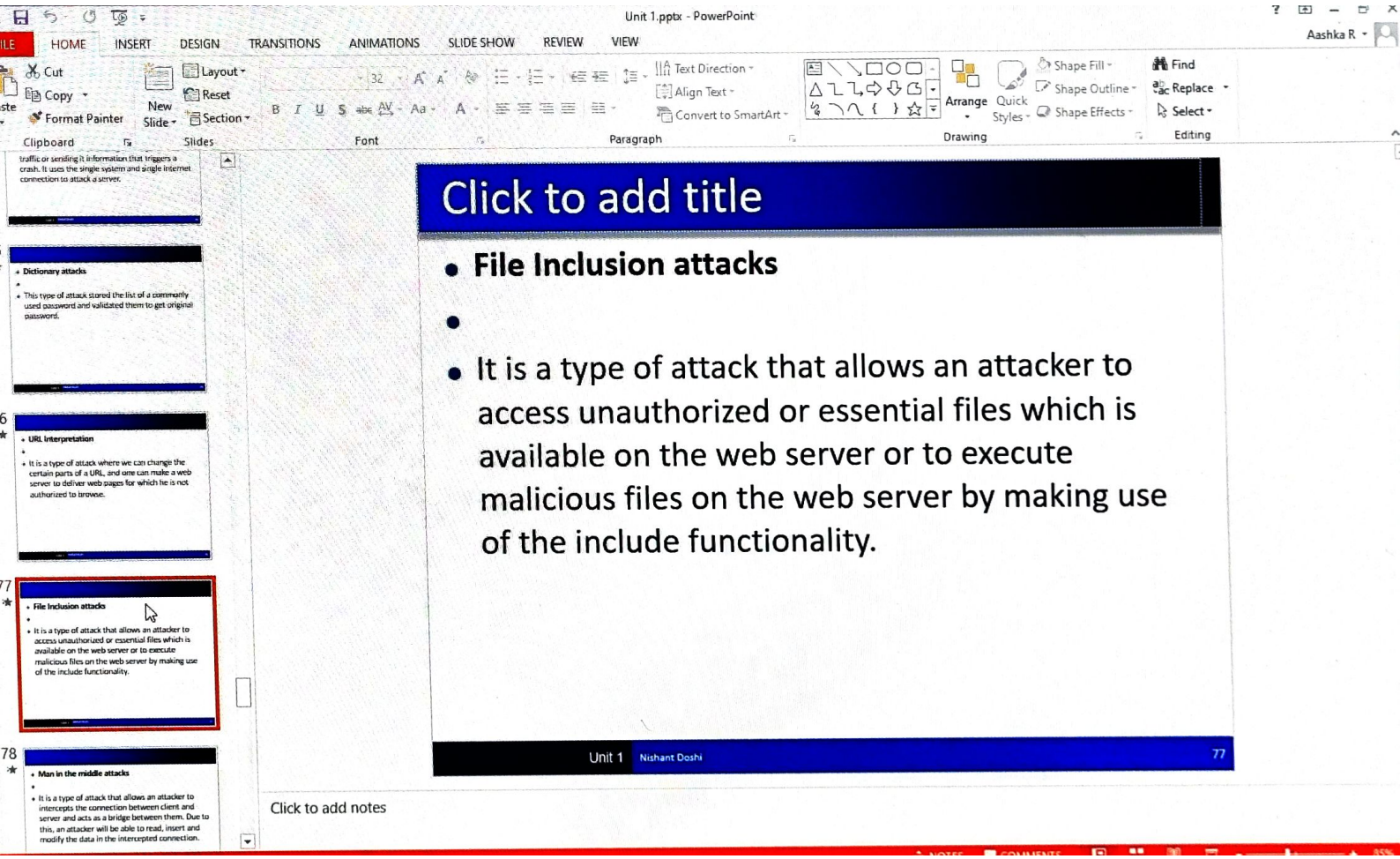

Unit 1.pptx - PowerPoint
FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Aashka R
Cut
Copy
Format Painter
Paste
New Slide
Layout
Reset
Section
Text Direction
Align Text
Convert to SmartArt
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Find
Replace
Select
Clipboard
Slides
Font
Paragraph
Drawing
Editing
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. It uses the single system and single internet connection to attack a server.
75
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.
Unit 1
Nishant Doshi
72
Click to add notes
SLIDE 72 OF 96
ENGLISH (INDIA)
NOTES
COMMENTS
85%
Type here to search
ENG
13:38

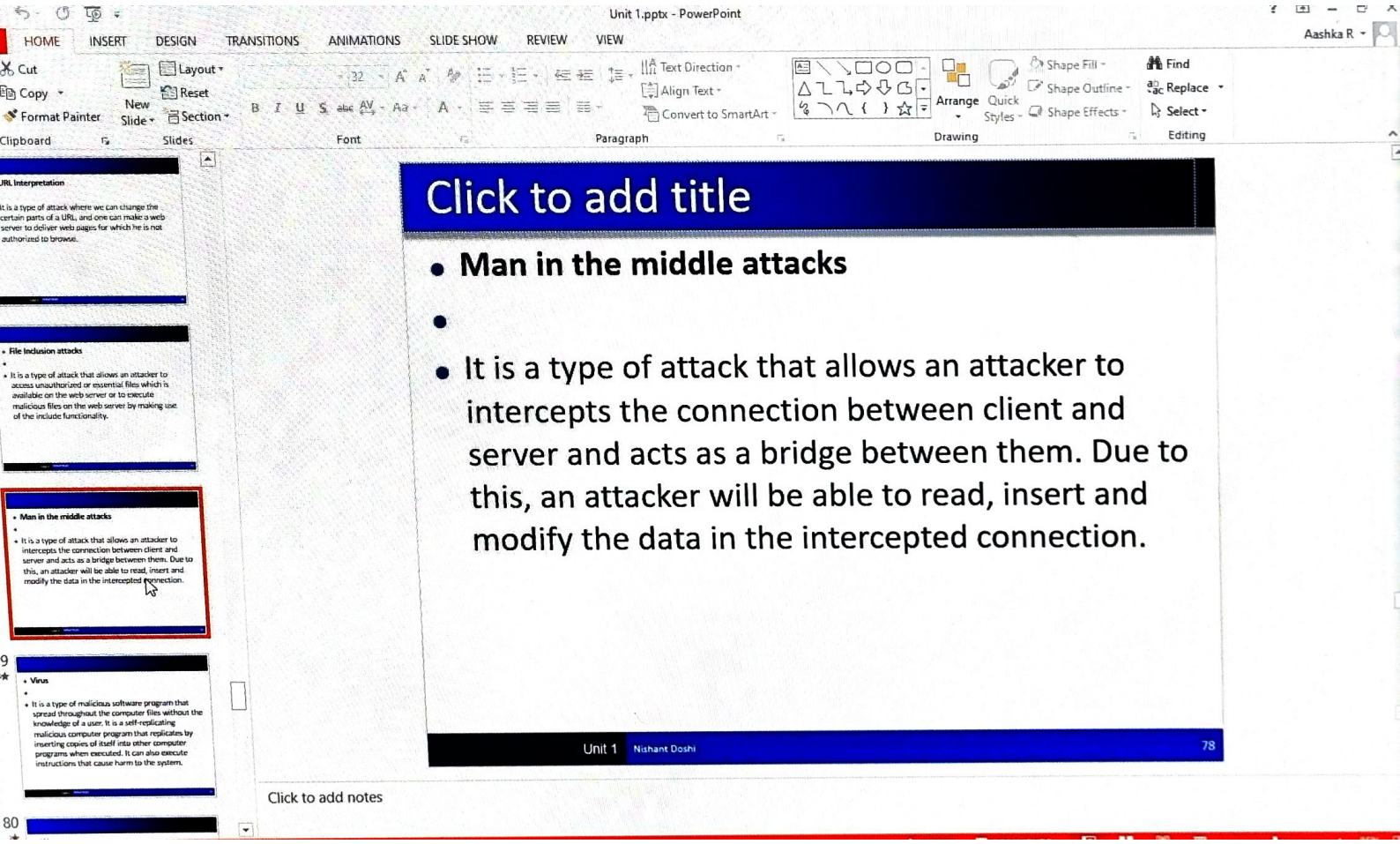

Unit 1.pptx - PowerPoint
FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Aashka R
Cut
Copy
Format Painter
Paste
Layout
Reset
Section
New Slide
Clipboard
Slides
Font
Paragraph
Text Direction
Align Text
Convert to SmartArt
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Drawing
Find
Replace
Select
Editing
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. It uses the single system and single internet connection to attack a server.
75
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
Click to add notes
NOTES
COMMENTS

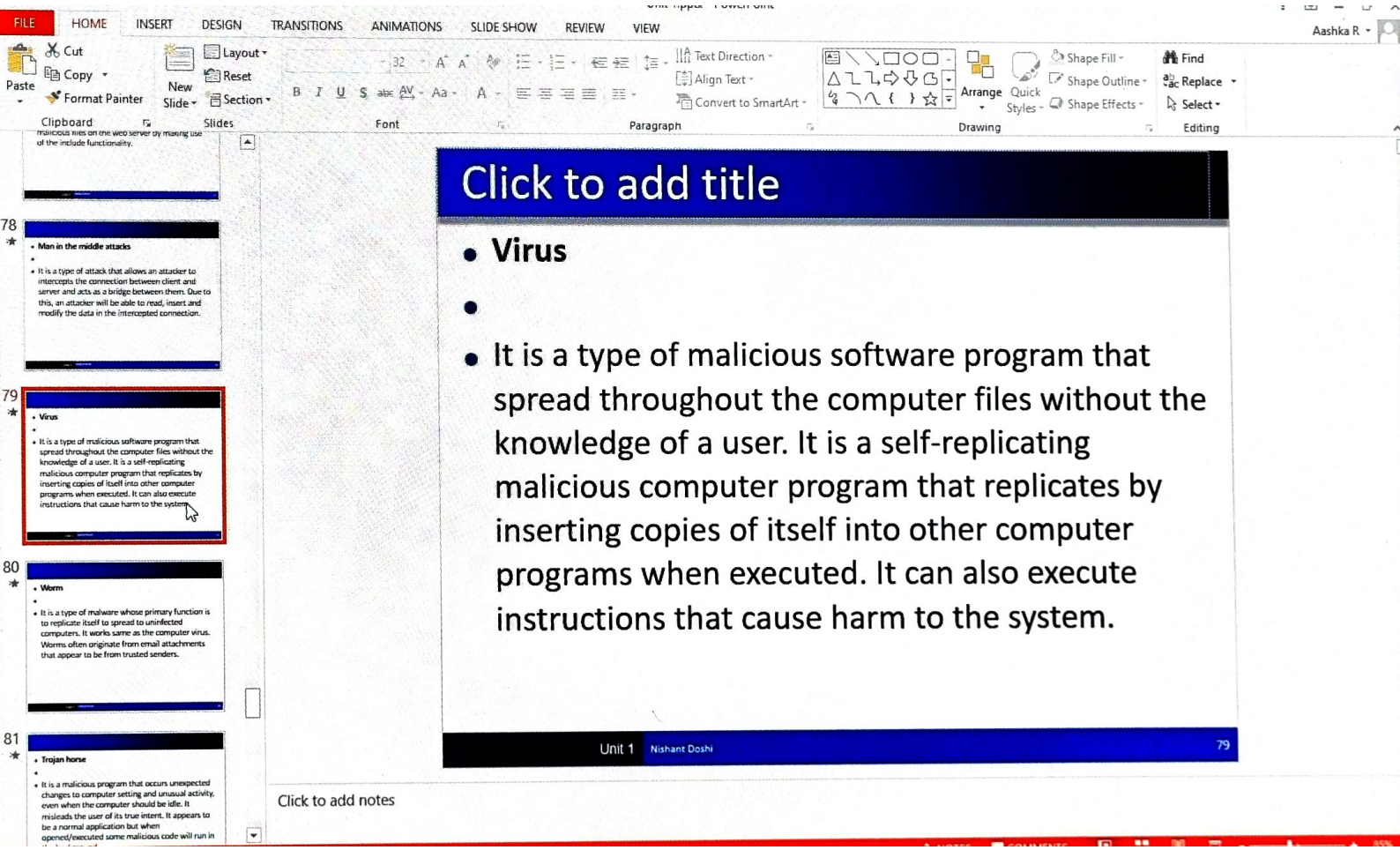

Unit 1.pptx - PowerPoint
FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Aashka R
Cut
Copy
Format Painter
Paste
Layout
Reset
Section
New Slide
Clipboard
Slides
Font
Text Direction
Align Text
Convert to SmartArt
Paragraph
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Drawing
Find
Replace
Select
Editing
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. 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

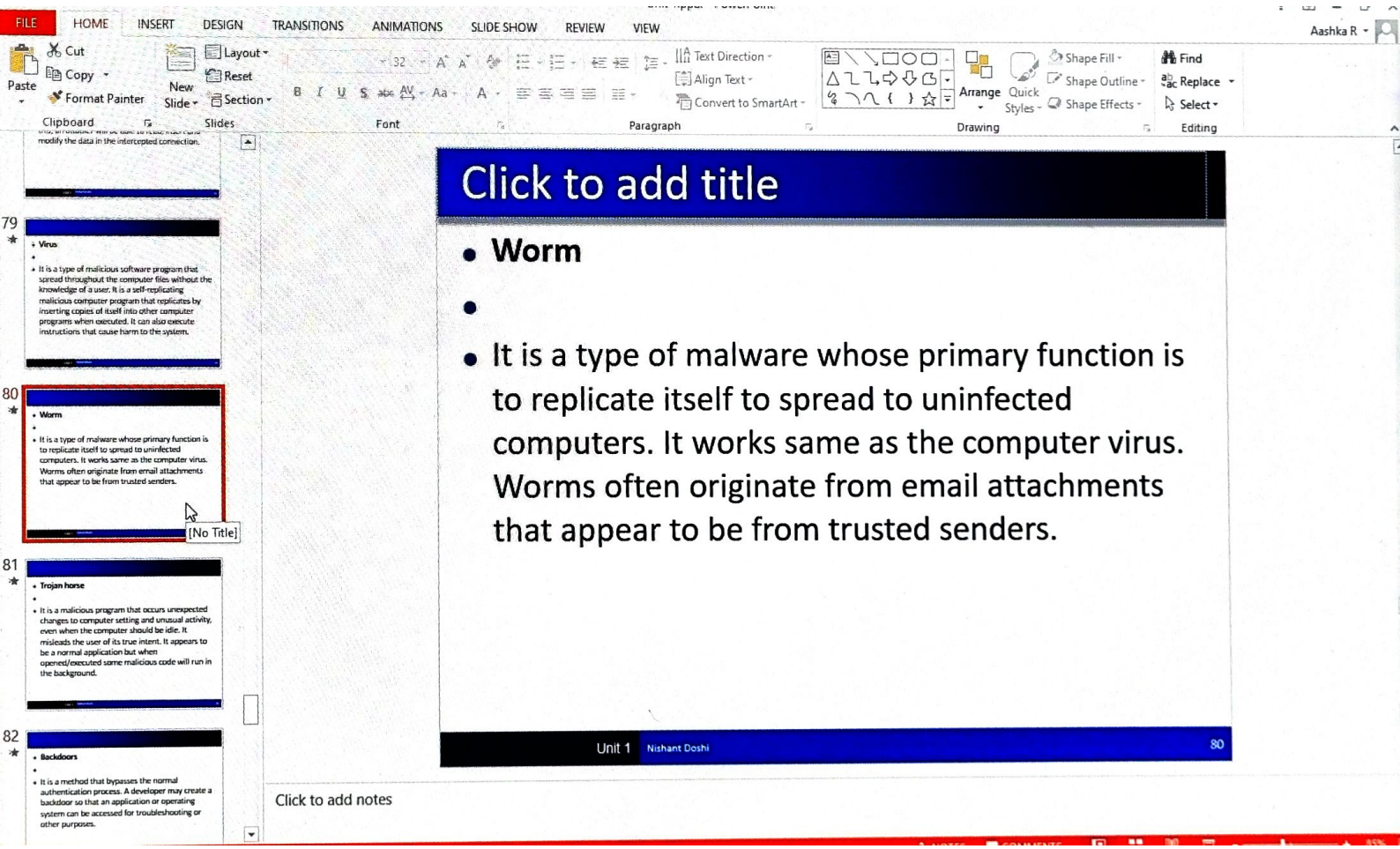

Unit 1.pptx - PowerPoint
Aashka R
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Cut
Copy
Format Painter
New Slide
Layout
Reset
Section
Text Direction
Align Text
Convert to SmartArt
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Find
Replace
Select
Clipboard
Slides
Font
Paragraph
Drawing
Editing
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 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
Dictionary attacks
This type of attack stored the list of a commonly used password and validated them to get original password.
Unit 1
Nishant Doshi
75
Click to add notes

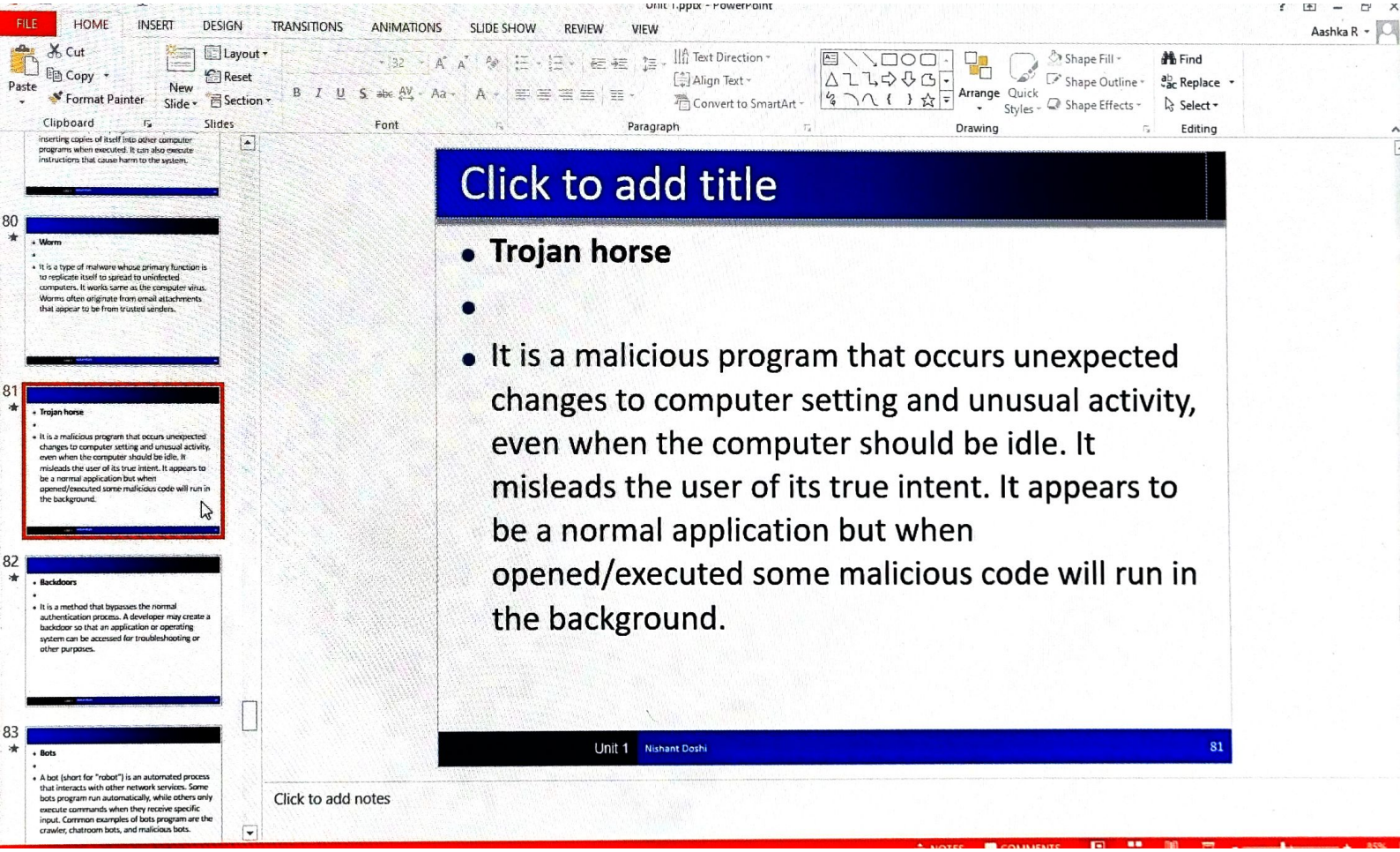

Unit 1.pptx - PowerPoint
Aashka R
FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Cut
Copy
Format Painter
Paste
New Slide
Layout
Reset
Section
Text Direction
Align Text
Convert to SmartArt
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Find
Replace
Select
Clipboard
Slides
Font
Paragraph
Drawing
Editing
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
[No 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.
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.
Unit 1
Nishant Doshi
76
Click to add notes

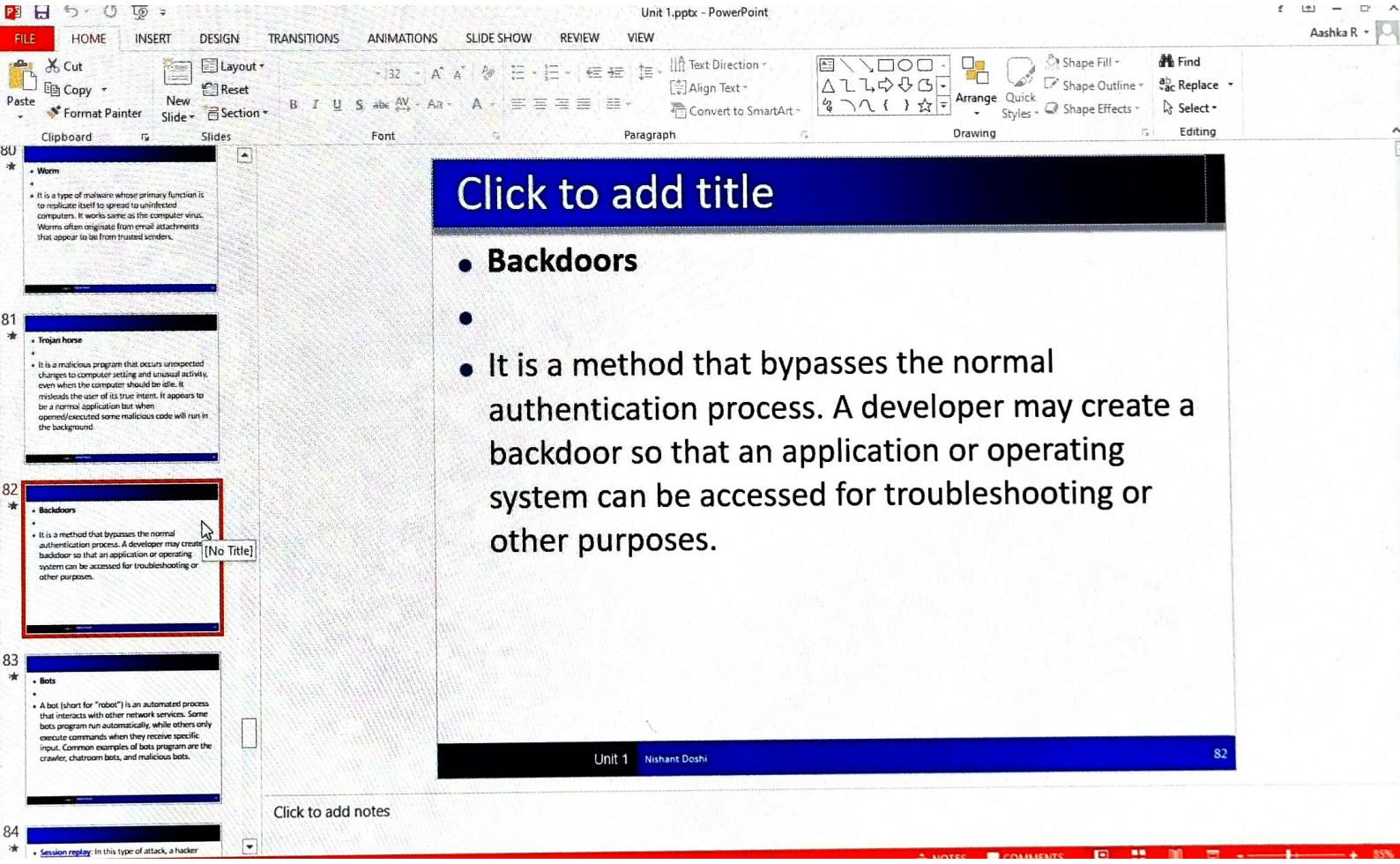

Unit 1.pptx - PowerPoint
Aashka R
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Cut
Copy
Format Painter
New Slide
Layout
Reset
Section
Text Direction
Align Text
Convert to SmartArt
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Find
Replace
Select
Clipboard
Slides
Font
Paragraph
Drawing
Editing
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.
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 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
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.
Unit 1
Nishant Doshi
77
Click to add notes

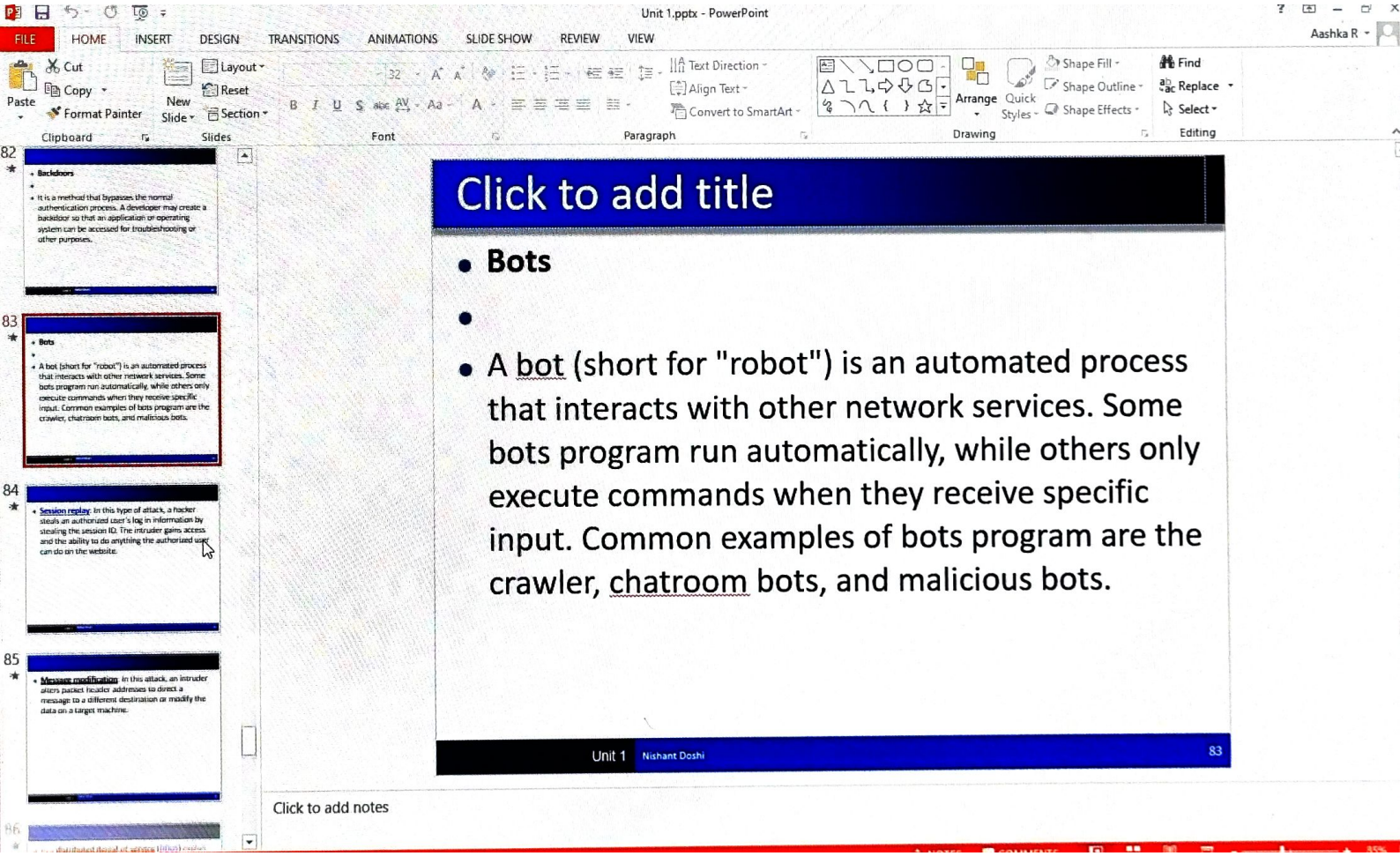

Unit 1.pptx - PowerPoint
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Aashka R
Cut
Copy
Format Painter
New Slide
Layout
Reset
Section
Text Direction
Align Text
Convert to SmartArt
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Find
Replace
Select
Clipboard
Slides
Font
Paragraph
Drawing
Editing
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.
Unit 1
Nishant Doshi
78
Click to add notes

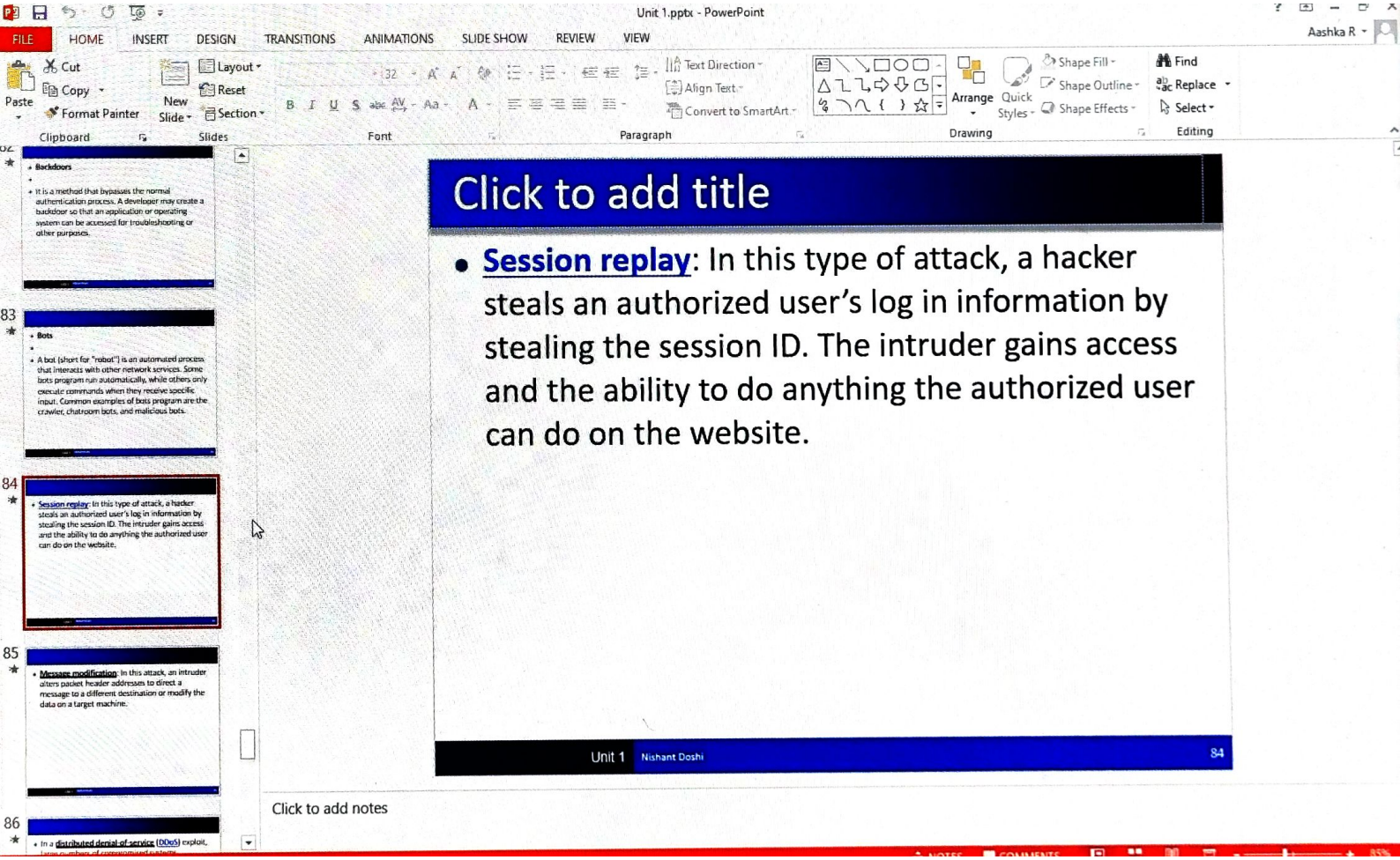

FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Aashka R
Cut
Copy
Format Painter
Paste
New Slide
Layout
Reset
Section
Clipboard
Slides
Text Direction
Align Text
Convert to SmartArt
Font
Paragraph
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Drawing
Find
Replace
Select
Editing
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.
79
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.
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
Click to add title
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.
Unit 1
Nishant Doshi
79
Click to add notes

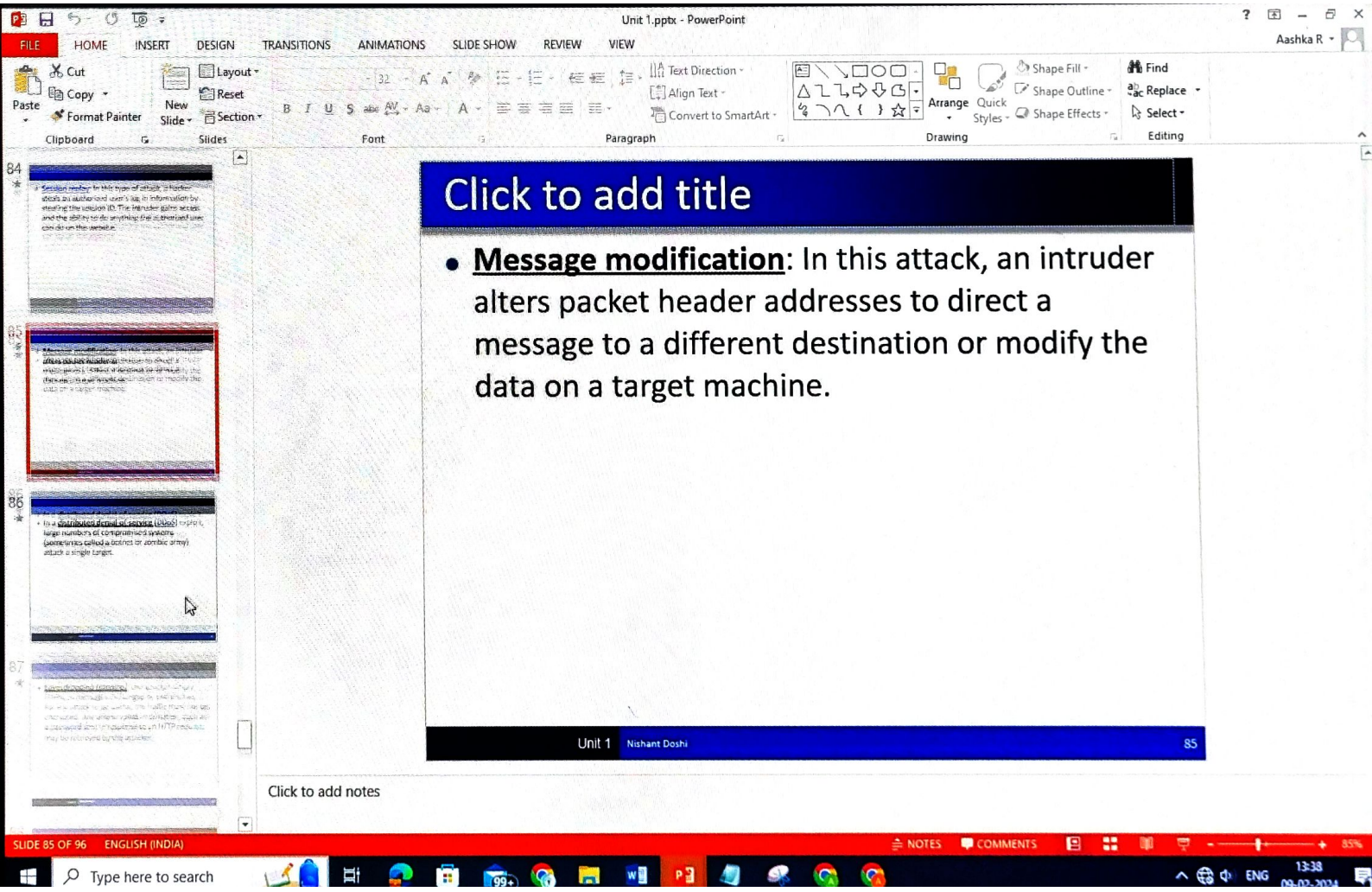

FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Aashka R
Cut
Copy
Format Painter
Paste
Layout
Reset
New Slide
Section
Clipboard
Slides
Font
Text Direction
Align Text
Convert to SmartArt
Paragraph
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Drawing
Find
Replace
Select
Editing
modify the data in the intercepted connection.
79
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.
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.
[No Title]
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.
Click to add title
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.
Unit 1
Nishant Doshi
80
Click to add notes

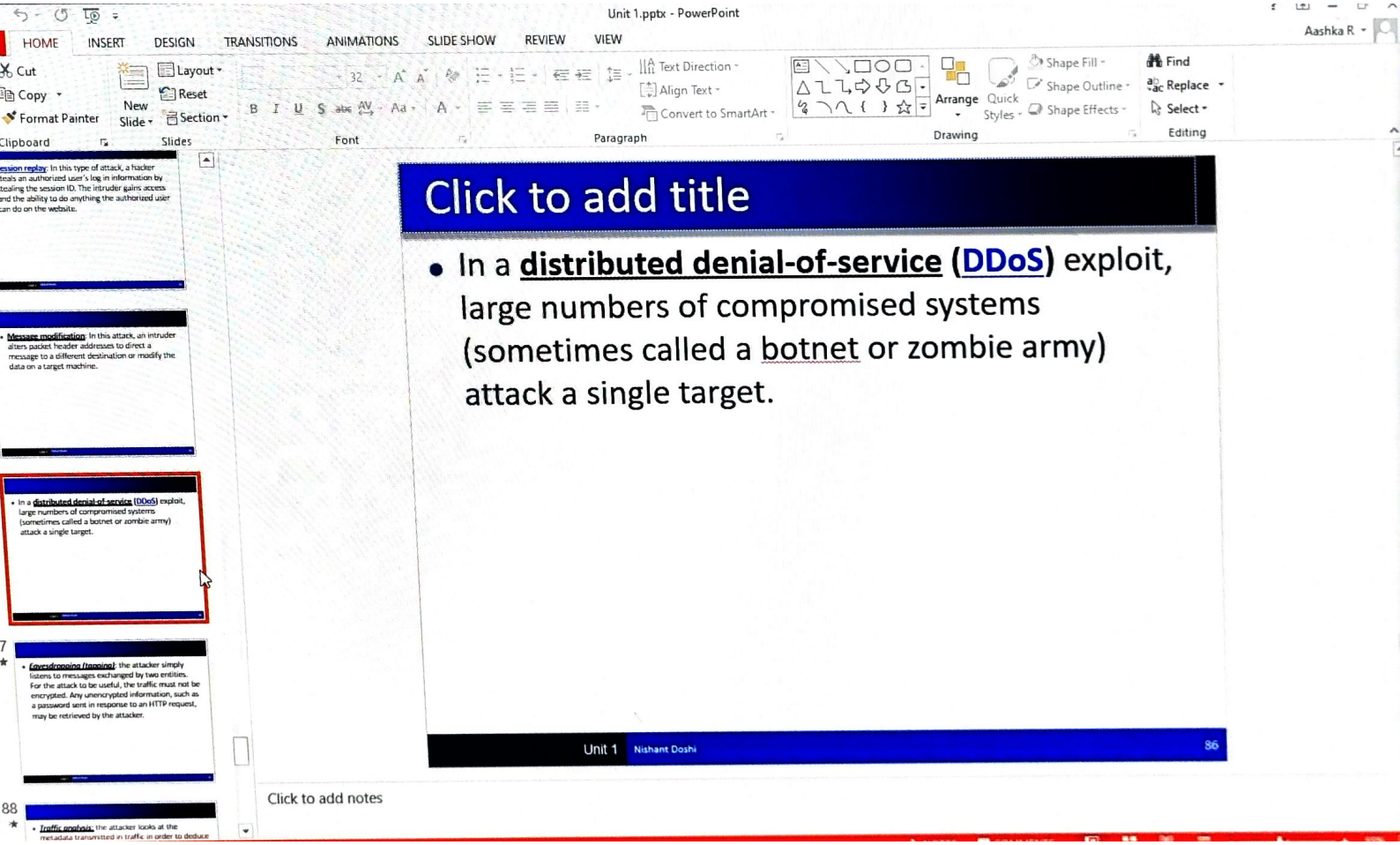

FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Aashka R
Paste
Cut
Copy
Format Painter
New Slide
Layout
Reset
Section
Text Direction
Align Text
Convert to SmartArt
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Find
Replace
Select
Clipboard
Slides
Font
Paragraph
Drawing
Editing
inserting copies of itself into other computer programs when executed. It can also execute instructions that cause harm to the system.
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.
Unit 1
Nishant Doshi
81
Click to add notes

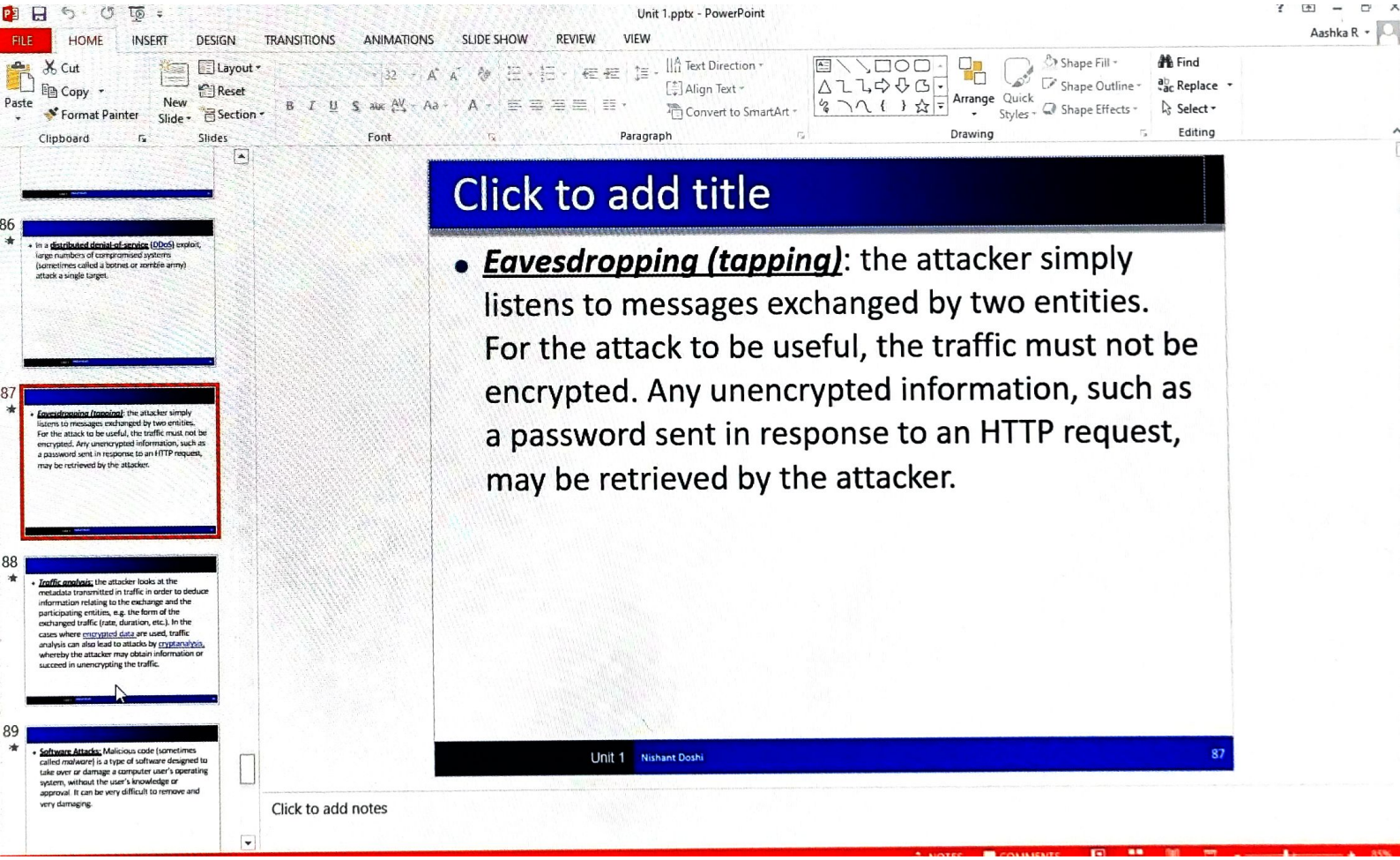

Unit 1.pptx - PowerPoint
FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Aashka R
Cut
Copy
Format Painter
Paste
Clipboard
New Slide
Layout
Reset
Section
Slides
Text Direction
Align Text
Convert to SmartArt
Paragraph
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Drawing
Find
Replace
Select
Editing
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.
[No Title]
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

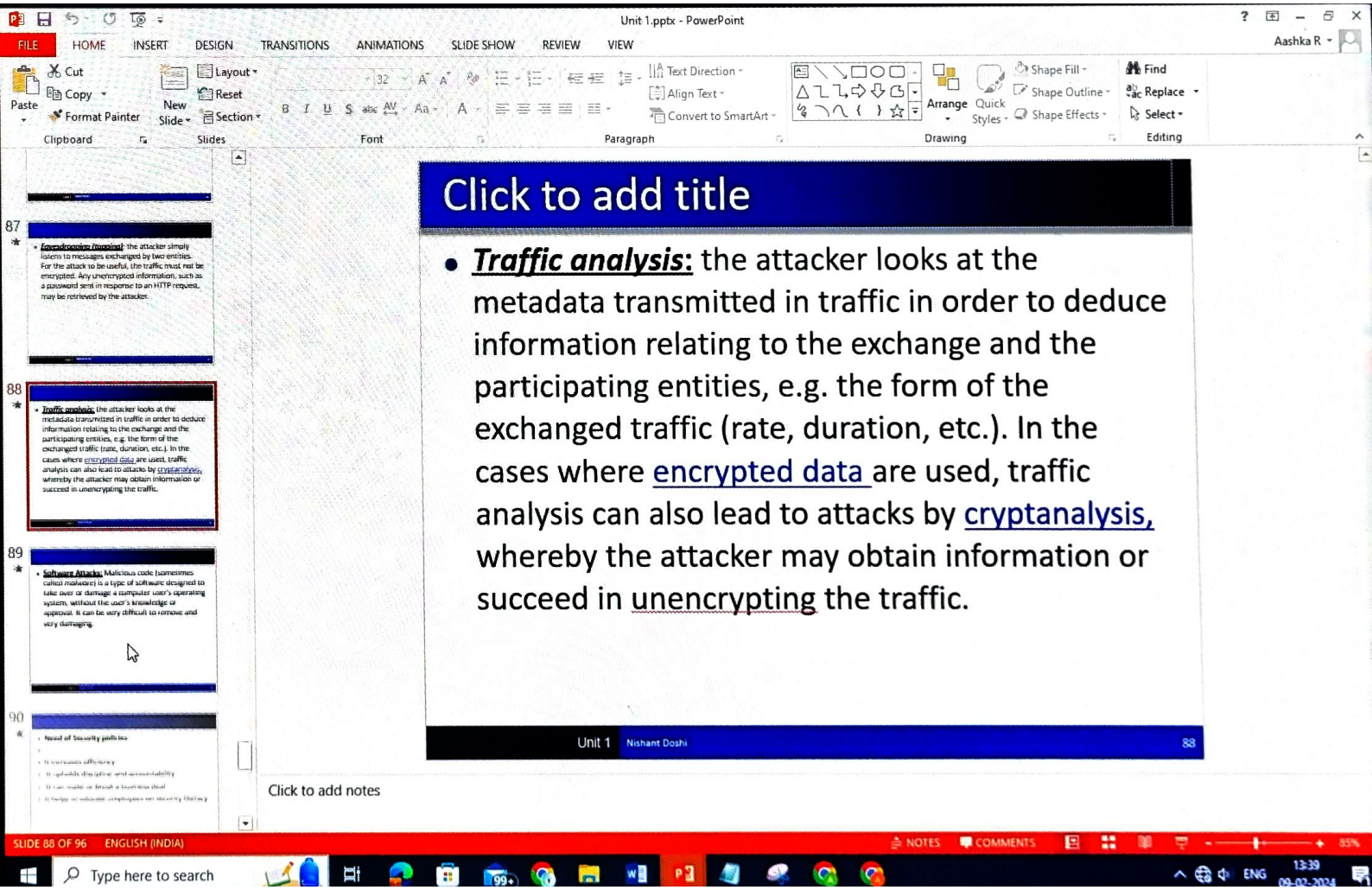

Unit 1.pptx - PowerPoint
Aashka R
FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Paste
Cut
Copy
Format Painter
New Slide
Layout
Reset
Section
Text Direction
Align Text
Convert to SmartArt
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Find
Replace
Select
Clipboard
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.
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.
Unit 1
Nishant Doshi
83
Click to add notes

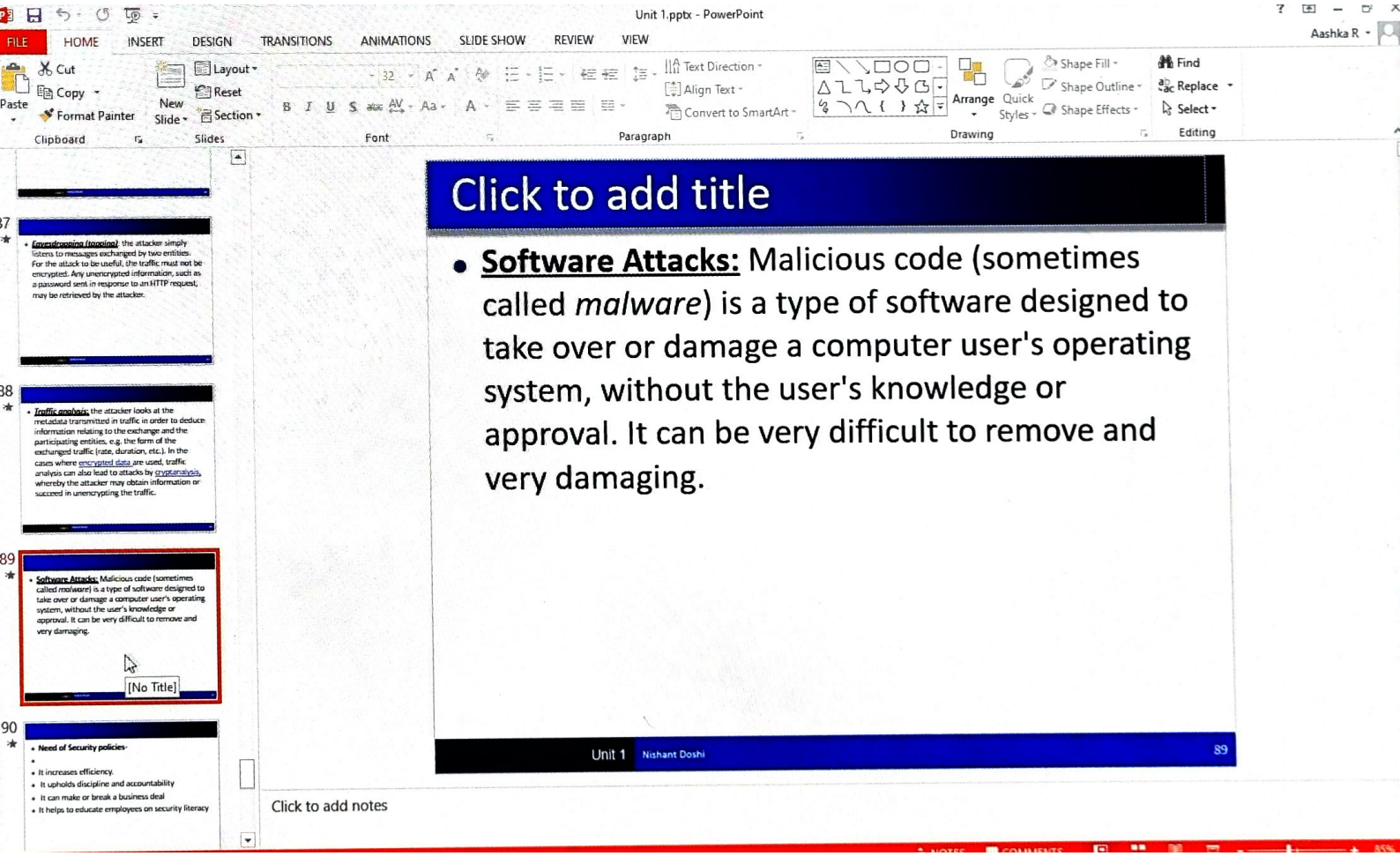

Unit 1.pptx - PowerPoint
Aashka R
FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Cut
Copy
Format Painter
Paste
New Slide
Layout
Reset
Section
Text Direction
Align Text
Convert to SmartArt
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Find
Replace
Select
Clipboard
Slides
Font
Paragraph
Drawing
Editing
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
In a distributed denial of service (DDoS) exploit,
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.
Unit 1
Nishant Doshi
84
Click to add notes

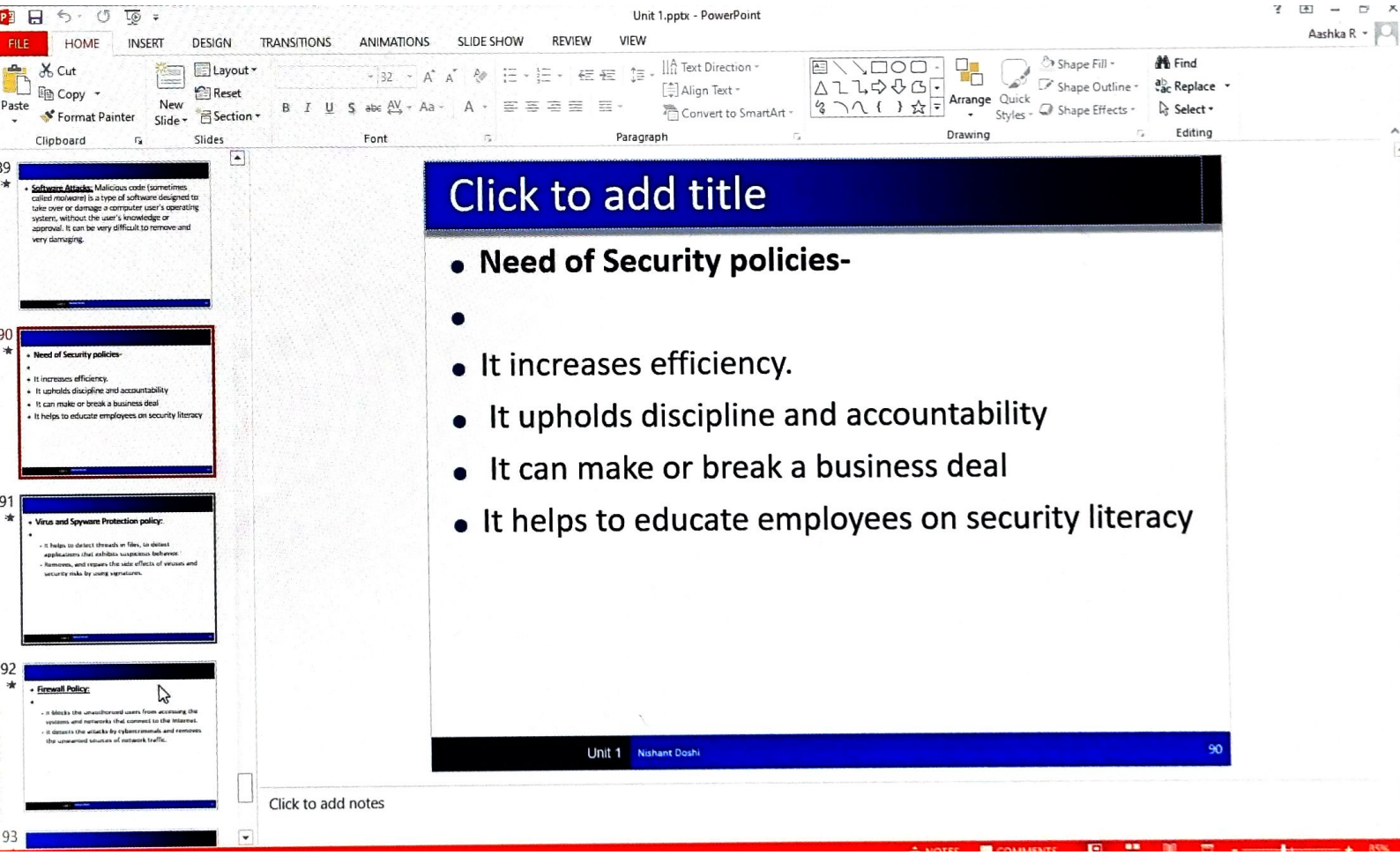

Unit 1.pptx - PowerPoint
Aashka R
FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Paste
Cut
Copy
Format Painter
New Slide
Layout
Reset
Section
Text Direction
Align Text
Convert to SmartArt
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Find
Replace
Select
Clipboard
Slides
Font
Paragraph
Drawing
Editing
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)
NOTES
COMMENTS
85%
Type here to search
ENG
13:38
09-02-2024

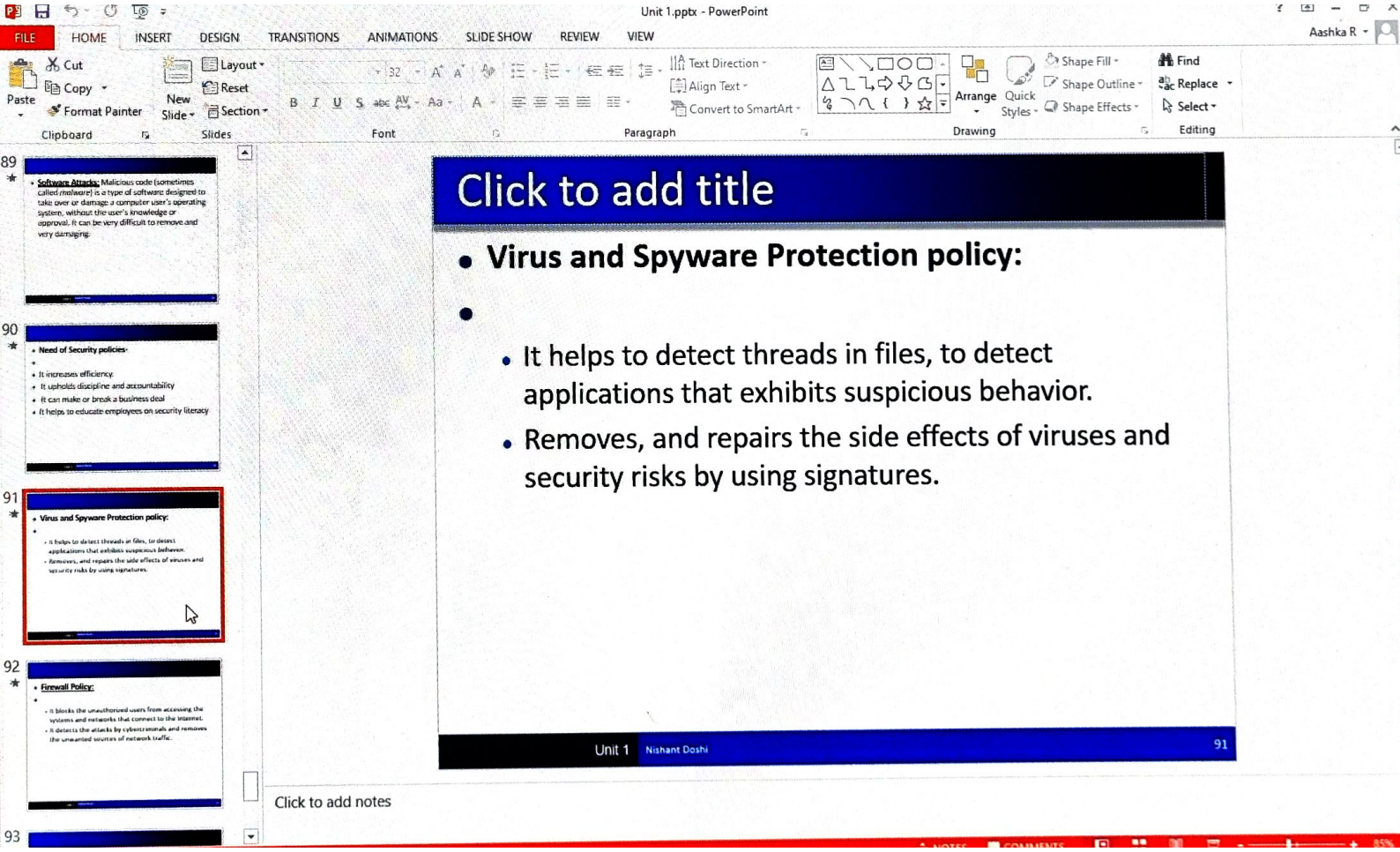

Unit 1.pptx - PowerPoint
Aashka R
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Cut
Copy
Format Painter
New Slide
Layout
Reset
Section
Text Direction
Align Text
Convert to SmartArt
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Find
Replace
Select
Clipboard
Slides
Font
Paragraph
Drawing
Editing
Click to add title
In a distributed denial-of-service (DDoS) exploit, large numbers of compromised systems (sometimes called a botnet or zombie army) attack a single target.
Unit 1
Nishant Doshi
86
Click to add notes

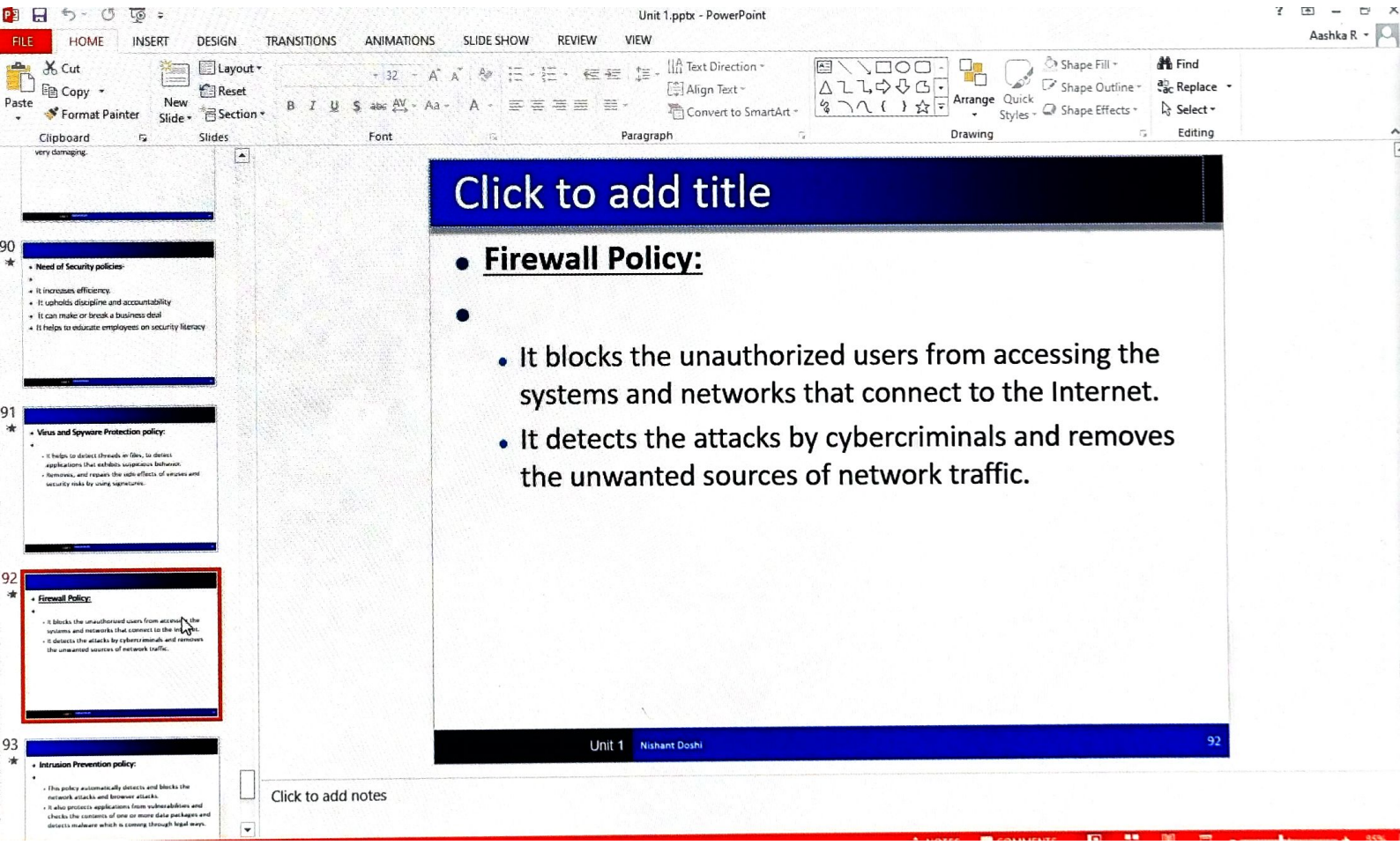

Unit 1.pptx - PowerPoint
Aashka R
FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Cut
Copy
Format Painter
Paste
New Slide
Layout
Reset
Section
Clipboard
Slides
Font
Text Direction
Align Text
Convert to SmartArt
Paragraph
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Drawing
Find
Replace
Select
Editing
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 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 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 title
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.
Unit 1
Nishant Doshi
87
Click to add notes

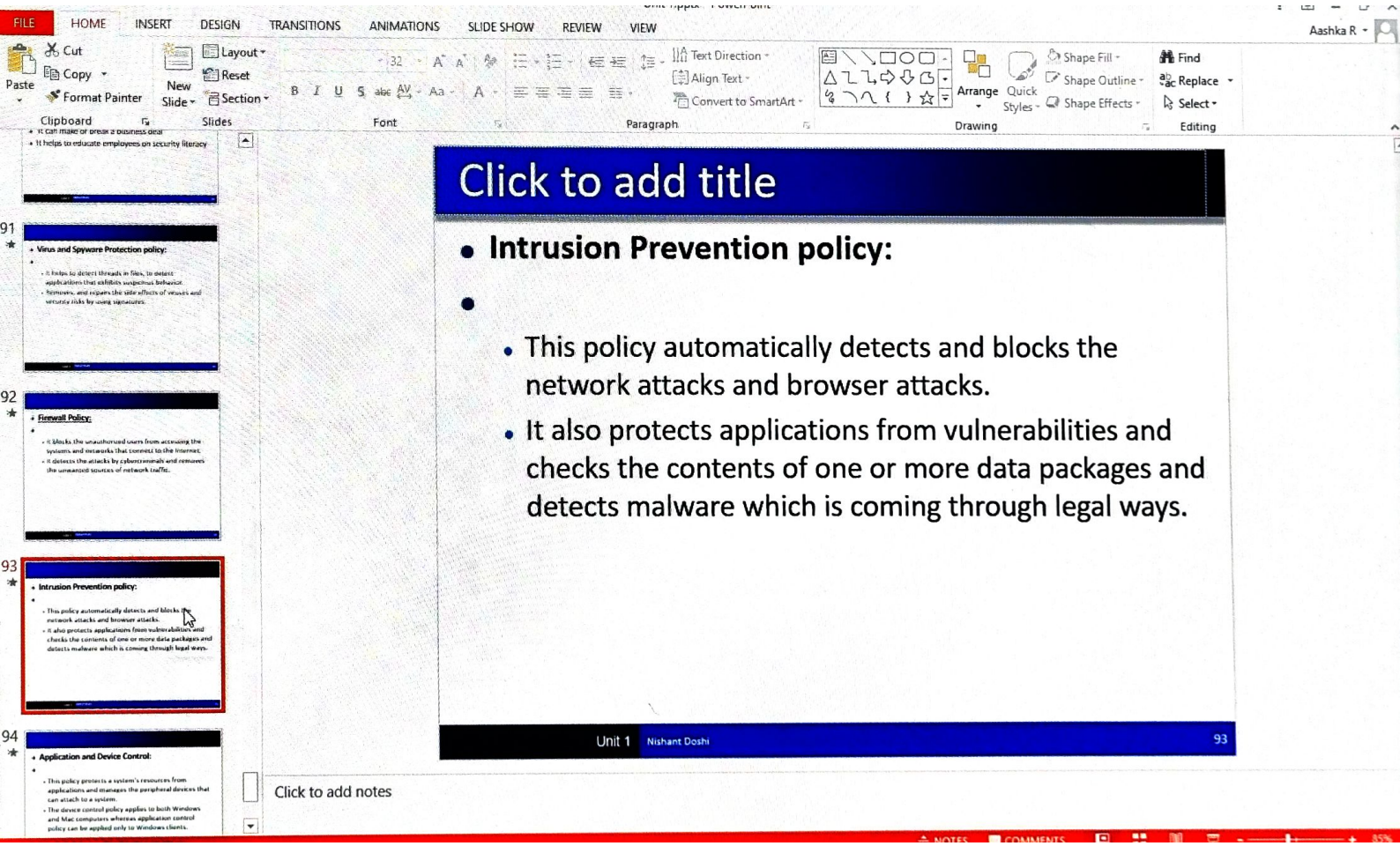

Unit 1.pptx - PowerPoint
FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Aashka R
Cut
Copy
Format Painter
Paste
Layout
Reset
New Slide
Section
Text Direction
Align Text
Convert to SmartArt
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Find
Replace
Select
Clipboard
Slides
Font
Paragraph
Drawing
Editing
87
Eavesdropping (Sniffing): 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 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 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
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)
NOTES
COMMENTS
85%
Type here to search
ENG
13:39
09-02-2024

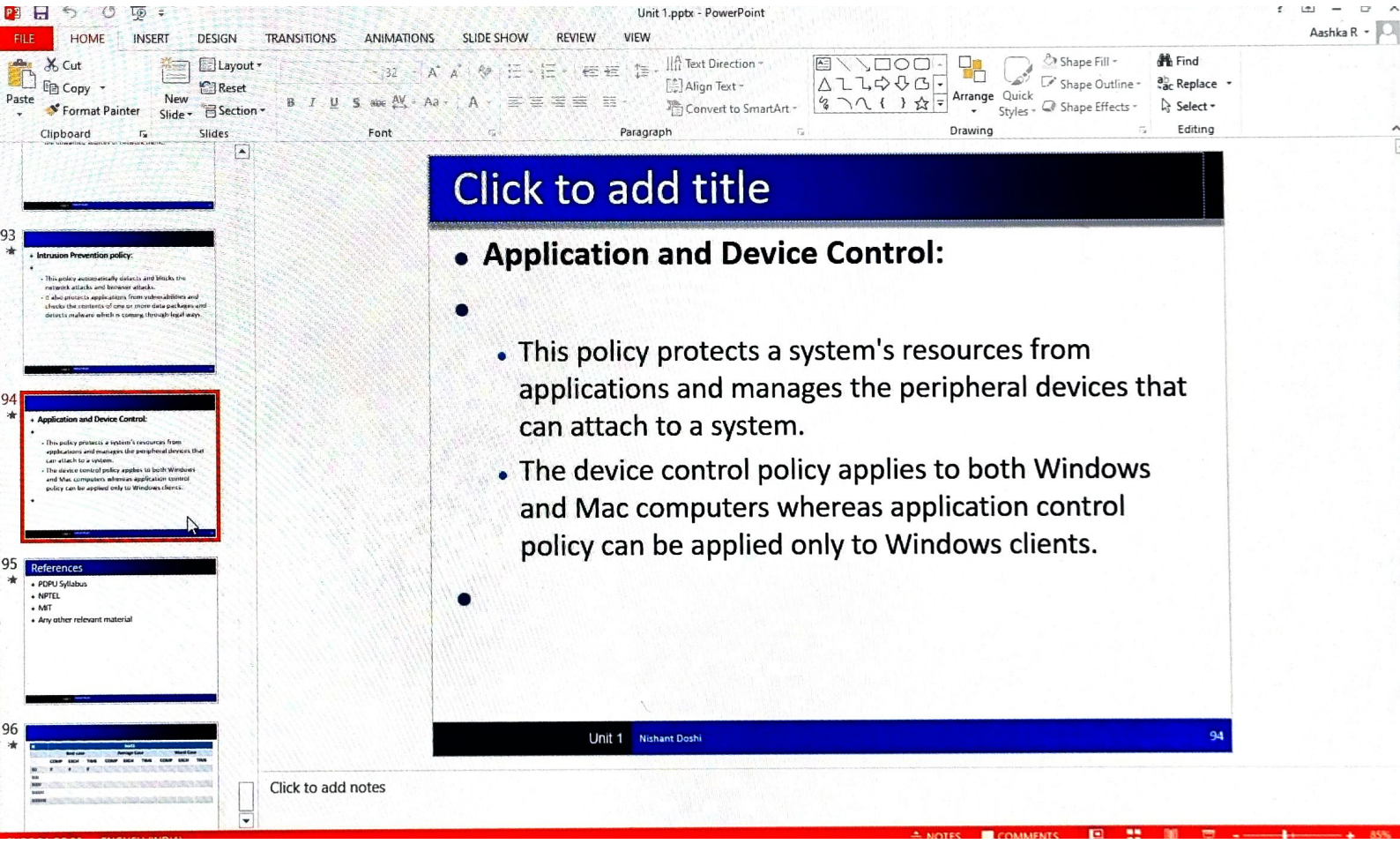

Unit 1.pptx - PowerPoint
Aashka R
FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Cut
Copy
Format Painter
Paste
New Slide
Layout
Reset
Section
Clipboard
Slides
Font
Text Direction
Align Text
Convert to SmartArt
Paragraph
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Drawing
Find
Replace
Select
Editing
Click to add title
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.
Unit 1
Nishant Doshi
89
Click to add notes
[No Title]
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

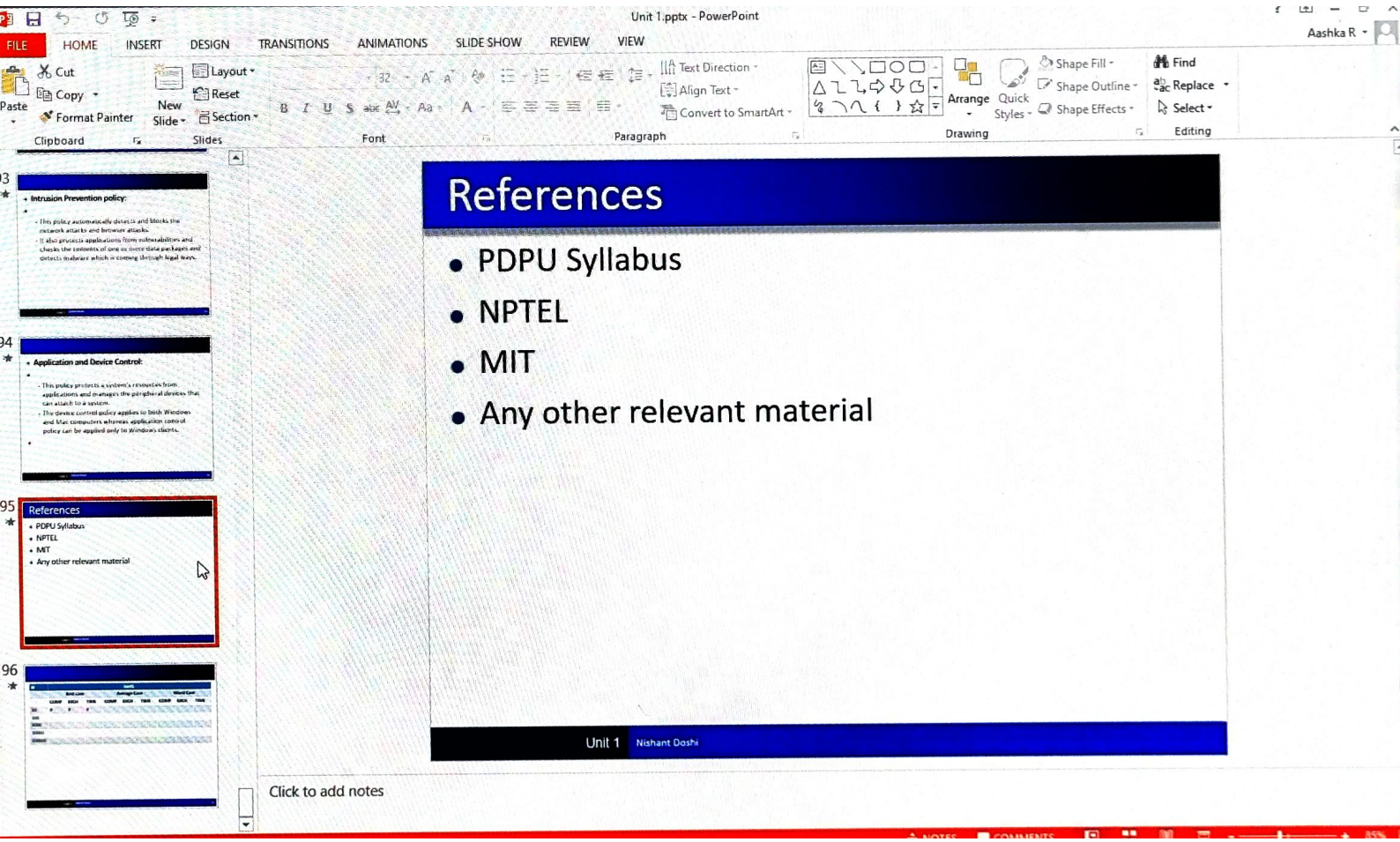

Unit 1.pptx - PowerPoint
Aashka R
FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Cut
Copy
Format Painter
Paste
New Slide
Layout
Reset
Section
Clipboard
Slides
Font
Text Direction
Align Text
Convert to SmartArt
Paragraph
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Drawing
Find
Replace
Select
Editing
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:
92
Firewall Policy:
93
Click to add title
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
Unit 1
Nishant Doshi
90
Click to add notes

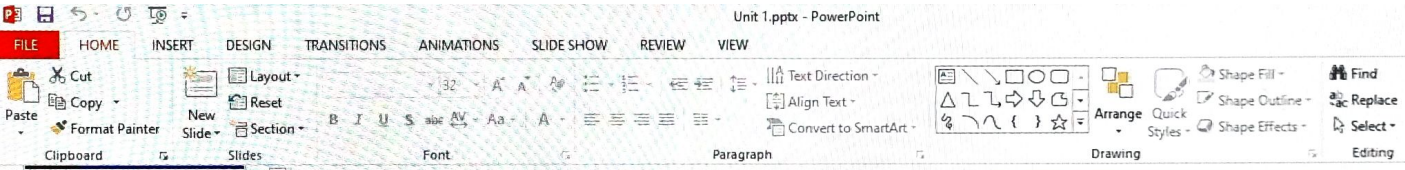

Unit 1.pptx - PowerPoint
FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Aashka R
Cut
Copy
Format Painter
Paste
Layout
Reset
Section
New Slide
Clipboard
Slides
Font
Text Direction
Align Text
Convert to SmartArt
Paragraph
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Drawing
Find
Replace
Select
Editing
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 cybercriminals 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

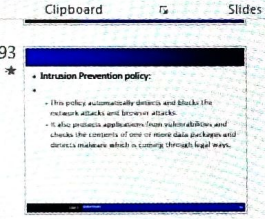

Unit 1.pptx - PowerPoint
FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Aashka R
Cut
Copy
Format Painter
Paste
New Slide
Layout
Reset
Section
Text Direction
Align Text
Convert to SmartArt
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Find
Replace
Select
Clipboard
Slides
Font
Paragraph
Drawing
Editing
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 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

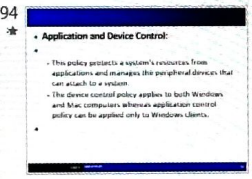

FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Aashka R
Cut
Copy
Format Painter
Paste
Layout
Reset
New Slide
Section
Clipboard
Slides
Font
Text Direction
Align Text
Convert to SmartArt
Paragraph
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Drawing
Find
Replace
Select
Editing
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 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.
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.
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

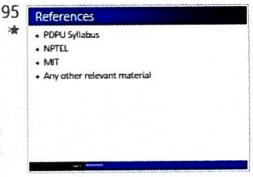

Unit 1.pptx - PowerPoint
FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Aashka R
Cut
Copy
Format Painter
Paste
Layout
Reset
New Slide
Section
Clipboard
Slides
Font
Text Direction
Align Text
Convert to SmartArt
Paragraph
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Drawing
Find
Replace
Select
Editing
93
Intrusion Prevention policy:
94
Application and Device Control:
95
References
PDPU Syllabus
NPTEL
MIT
Any other relevant material
96
Click to add title
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.
Unit 1
Nishant Doshi
94
Click to add notes
NOTES
COMMENTS

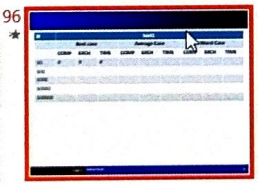

Unit 1.pptx - PowerPoint
Aashka R
FILE
HOME
INSERT
DESIGN
TRANSITIONS
ANIMATIONS
SLIDE SHOW
REVIEW
VIEW
Cut
Copy
Format Painter
Paste
New Slide
Layout
Reset
Section
Clipboard
Slides
Font
Text Direction
Align Text
Convert to SmartArt
Paragraph
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Drawing
Find
Replace
Select
Editing
93
Intrusion Prevention policy:
94
Application and Device Control:
95
References
PDPU Syllabus
NPTEL
MIT
Any other relevant material
96
References
PDPU Syllabus
NPTEL
MIT
Any other relevant material
Unit 1
Nishant Doshi
Click to add notes











Click to add title

N	Sort1								
	Best case			Average Case			Worst Case		
	COMP	EXCH	TIME	COMP	EXCH	TIME	COMP	EXCH	TIME
10	#	#	#						
100									
1000									
10000									
100000									

Click to add notes