

Cyber Security Intro

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

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Paste Format Painter New Slide Section Clipboard Slides Font Paragraph Drawing 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 or global network available.

Security means ways to provide protection to these data that are available on internet.

Definition of Cybersecurity:

Practice of protecting computers, networks, programs from Digital 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

SIDE 5 OF 96 ENGLISH (INDIA)

Type here to search

Unit 1 Nishant Doshi

Click to add notes

NOTES COMMENTS

Virus



Unit 1.pptx - PowerPoint

Aashka R

Warning bells for Virus

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

Click to add notes

Unit 1 Nishant Doshi

Unit 1.pptx - PowerPoint

Ashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

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

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.

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.

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.

Types of Hackers

- There are three types of hacker:
 - White Hat Hacker: It involves performing a security evaluation and testing with complete knowledge of the system.
 - Gray Hat Hacker: It involves performing a security evaluation and testing without complete knowledge of the system.
 - Black Hat Hacker: Testing with no prior knowledge of the network infrastructure or systems.

Click to add notes

Unit 1 Nishant Doshi

NOTES COMMENTS

Unit 1.pptx - PowerPoint

Aashka R

File Home Insert Design Transitions Animations Slide Show Review View

Cut Copy Format Painter Paste New Slide Section Layout Reset

Virus

- A computer virus is a program that can copy itself and spread from one computer to another without the permission or knowledge of the user.
- A computer virus has 2 major characteristics:
 - The ability to replicate itself
 - The ability to spread to another computer file

Warning bells for Virus

- Frequent pop-up windows.
- Most 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.

Hacker and Hacking

HACKING is the practice of gaining access to a computer system without the owner's permission. It can be used for various purposes such as stealing data or maliciously damage the computer.

- A "hacker" is a person skilled in computer systems who uses their knowledge to find ways to overcome an obstacle within a computerized system by understanding its weaknesses.
- Sometimes the hacker utilizes their technical know-how of how a system works to gain access and steal data which would otherwise not be accessible in that.

Types of Hackers

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

Unit 1 Nishant Doshi

Click to add notes

NOTES COMMENTS

Unit 1.pptx - PowerPoint

Aashka R

Types of Hacking

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



Unit 1 Nishant Doshi

Click to add notes

9

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste New Slide Section Reset Layout Section

Clipboard Slides

Font Paragraph

Drawing Editing

Find Replace Select

Text Direction Align Text Convert to SmartArt

Shapes Quick Styles Shape Effects

9 Types of Hacking

- Website Hacking: Web hacking refers to exploitation of applications via HTTP which can be used to manipulate 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 keylogging.



12 Social Engineering

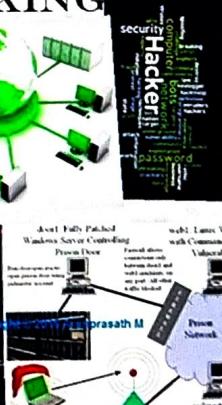
- Social engineering is an attempt to urge you to share personal info; sometimes by impersonating a trustworthy supply.



Click to add title

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

NETWOR
HACKING



Unit 1 Nishant Doshi

Click to add notes

10

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste New Slide Section Layout Reset

Clipboard Slides

Font Paragraph Drawing Editing

Find Replace Select

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 involves gathering information about domain by using tools like:
 - Telnet
 - netcat
 - nmap
 - ping
 - traceroute

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 source.

13

Click to add title

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



Unit 1 Nishant Doshi

11

Click to add notes

Unit 1.pptx - PowerPoint

Aashka R

LE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Reset Layout Reset

Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Effects

Find Replace Select

Types of Hacking

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

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

- fofu
- medit
- enum4l
- nmap
- traceroute

1 • 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.

Click to add title

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

Unit 1 Nishant Doshi

Click to add notes

NOTES COMMENTS

85%

Unit 1.pptx - PowerPoint

Aashka R

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

Cut Copy Format Painter New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Effects

Find Replace Select

Click to add title

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

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

14 • Malware

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

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

15 Malware (Contd.)

Types:

- Viruses
- Trojan Horse
- Spyware
- Adware
- Worms

Click to add notes

Unit 1 Nishant Doshi

NOTES COMMENTS

85%

The image shows a Microsoft PowerPoint slide titled "Click to add title". The slide content includes a bullet point from slide 13 about "Phishing" and another bullet point from slide 14 about "Malware". On the left, there are thumbnail previews of previous slides. The ribbon at the top has tabs like File, Home, Insert, Design, Transitions, Animations, Slide Show, Review, and View. The status bar at the bottom right shows the slide number 85%.

Unit 1.pptx - PowerPoint

Aashka R -

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Reset Section

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.

Click to add notes

Unit 1 Nishant Doshi

The screenshot shows a Microsoft PowerPoint slide titled "Malware". The slide has a dark blue header and footer bar. The main content area has a white background. There are two bullet points in the list:

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

The slide is part of a presentation named "Unit 1.pptx" and is currently on slide 15. The footer of the slide displays the name "Nishant Doshi".

Unit 1.pptx - PowerPoint

Aashka R.

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Reset Section

Clipboard Slides

SOCIAL ENGINEERING

13

Phishing: In this type of hacking, Hackers intend to take advantage of user's like login password, MasterCard detail etc. For example, Hackers can make a replicating first website for users interaction and can steal critical information.

14

Malware

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

15

Malware (Contd.)

Types:

- Viruses
- Trojan Horse
- Spyware
- Adware
- Worms

16

INTERNET GOVERNANCE

WSIS FORUM 2023

Unit 1 Nishant Doshi

Click to add notes

NOTES COMMENTS

13:36 09-02-2024

SLIDE 15 OF 96 ENGLISH (INDIA)

Type here to search

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

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

14 Malware

Malware is malicious 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.

INTERNET GOVERNANCE

WSIS FORUM 2023

INTERNET GOVERNANCE

17 INTERNET GOVERNANCE

- Internet governance is the development and application by Governments, international organizations and local society of the principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet.

INTERNET GOVERNANCE

UNIT 1 Nishant Doshi

Click to add notes



15 Malware (Contd.)

- Types:
 - Viruses
 - Trojan Horse
 - Spamware
 - 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.



18 INTERNET GOVERNANCE
• In other word Internet is decentralized network of computers which are interconnected and organized to run 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.



19 SELF REGULATION
• Self regulation works in a process with steps:

Unit 1 Nishant Doshi

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

NOTES COMMENTS

Unit 1.pptx - PowerPoint

Aashka R

Cut Copy Format Painter New Slide Section 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) Prepared the milestones

WSIS FORUM 2023

17 INTERNET GOVERNANCE

• Internet governance is the development and application by:

- Government
- the private sector
- civil society

• in their respective roles, of shared principles, norms, rules, and agreed practices that ensure the evolution and use of the Internet.

IGF

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

- Click to add text
- 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.

19 SELF REGULATION

• Self regulation works in a group with strong

SLIDE 18 OF 96 ENGLISH (INDIA)

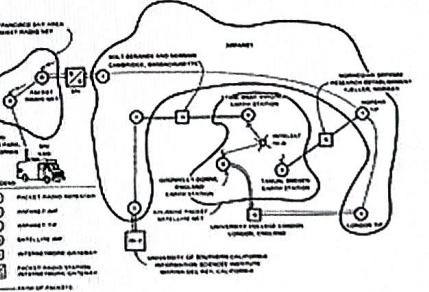
Click to add notes

Text Direction Align Text Convert to SmartArt

Shape Fill Shape Outline Quick Styles Shape Effects

Find Replace Select

13:37 ENG 22-03-2024



The diagram illustrates the ARPANET network, which was one of the early components that evolved into the Internet. It shows a central node labeled 'ARPA' connected to several other nodes, including 'SRI', 'BBN', 'UCB', 'UCSB', 'UCI', 'UCD', 'ISI', 'LBNL', 'UCLA', 'USC', 'SAC', 'NSFNET', 'CERNET', 'CHINANET', 'KOREANET', 'JAPANET', and 'EUROPEANET'. The network is depicted as a mesh of lines representing connections between nodes. A legend at the bottom left defines symbols for 'POINT-TO-POINT', 'POINT-TO-MULTIPOINT', 'MESH', 'INTER-ROUTE GATEWAY', and 'POINT-TO-POINT MULTIPLEXER'.

Unit 1.pptx - PowerPoint

Aashka R

FILE INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste Clipboard Slides

Layout New Slide Section

Font Paragraph

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Effects

Find Replace Select

Drawing Editing

7 INTERNET GOVERNANCE

- Internet governance is the development and application by governments, the private sector and civil society of relevant rules, norms, and procedures that shape the evolution and use of the Internet.

8 INTERNET GOVERNANCE

- In other words Internet is a decentralized network of computers and people who have agreed to follow certain rules to run the Internet. And in turn, we have our own set of rules.

9 SELF REGULATION

- ARIN.NET is one of the components which originally evolved in the Internet.

10 SELF REGULATION

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

11 Policy Making

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

12 CHALLENGES AND CONSTRAINTS

Click to add notes

Unit 1 Nishant Doshi

Aashka R

Unit 1.pptx - PowerPoint

HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

Policy Making

INTERNET GOVERNANCE

- In other word Internet is a decentralized network of computers which are interconnected. And so for internet we have to set some rules.
- ARINET is one of the companies which eventually produced to became the internet.

SELF REGULATION

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

Policy Making

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

CHALLENGES AND CONSTRAINTS

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

Unit 1 Nishant Doshi

Click to add notes

NOTES COMMENTS

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste New Slide Section Clipboard Slides

Font Paragraph Drawing 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 things are managed automatically.

20 Policy Making

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

21 CHALLENGES AND CONSTRAINTS

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

22 CHALLENGES AND CONSTRAINTS (Contd.)

- All Intelligence: It is an area of computer science which is the creation of intelligent machines that do work and react like humans. Some of the areas include natural language processing, machine learning, speech recognition, Learning, Planning, Problem solving, etc.
- Cloud Vulnerability: Servers architecture and application which depends on third party cloud provider or on a bank and services such as google cloud functions, Amazon web services (AWS) lambda, etc.

23 CYBER WARFARE

Click to add notes

Unit 1 Nishant Doshi

NOTES COMMENTS

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste Clipboard Slides

Font Paragraph Drawing Editing

Policy Making

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

CHALLENGES AND CONSTRAINTS

- Ransomware Revolution: Ransomware is a type of malware in which the data on a victim's computer is locked, and payment is demanded before theransomed data is unlocked.
- Blockchain Revolution: A blockchain is a database that stores data in the form of blocks. It is not managed by a central authority. It is a system of interconnected physical devices which can be accessible through the internet.

CHALLENGES AND CONSTRAINTS (Contd.)

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

CYBER WARFARE

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

Click to add notes

Unit 1 Nishant Doshi

NOTES COMMENTS

CHALLENGES AND CONSTRAINTS (Contd.)

CHALLENGES AND CONSTRAINTS

AI Expansion: It is an area of computer science which is the creation of intelligent machines that do work and react like humans. Some of the activities related to artificial intelligence include speech recognition, Learning, Planning, Problem-solving, etc.

Serverless Apps 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.

CYBER WARFARE

Cyber Warfare is internet based conflict involving politically motivated attacks on information systems.

It also involves the action by a nation-state or international organization to attack and attempt to damage another nation's computers and information.

Click to add notes

NOTES COMMENTS

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

UNIT 1.PPTX - PowerPoint Aashka R

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

CYBER WARFARE

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 a series of chained blocks.
- IoT Threats: It refers to threats that affect the security of interconnected physical devices which can be accessible through the internet.

22 CHALLENGES AND CONSTRAINTS (Contd.)

- AI Expansion: It is an area of computer science that involves the creation of intelligent machines that can perform tasks that typically require human intelligence. Activities related to artificial intelligence include speech recognition, learning, planning, problem solving, etc.
- Serverless Apps Vulnerability: Serverless architecture and apps is an application model designed to run code without managing the 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.

24 CYBER WARFARE Types

- 1) Espionage
- 2) Sabotage
- 3) Denial of Service Attack
- 4) Electrical Power Grid
- 5) Propaganda Attacks
- 6) Economic Disruption
- 7) Cyber 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

COPY PASTE CUT COPY FORMAT PAINTER NEW SLIDE SECTION LAYOUT RESET

CHALLENGES AND CONSTRAINTS (Contd.)

- AI Expansion: It is a type of computer science which is the creation of intelligent machines that do work and react like humans. Some of the common applications of AI include speech recognition, Learning, Planning, Problem solving, etc.
- Software-As-A-Service: Services architecture and apps is an application which depends on third party to run and host on a back end services like google cloud function, amazon web services (AWS) lambda, etc.

CYBER WARFARE

- Cyber Warfare is internet based conflict involving politically motivated attacks on infrastructure.
- 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 Types

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

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.

Types of Espionage

26 Sabotage

Click to add notes

Unit 1 Nishant Doshi

NOTES COMMENTS

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

CYBER WARFARE Types

- 1 Espionage
- 2 Sabotage
- 3 Denial of Service (DoS)
- 4 Denial of Service (DoS)
- 5 Denial of Service (DoS)
- 6 Denial of Service (DoS)
- 7 Denial of Service (DoS)
- 8 Denial of Service (DoS)
- 9 Denial of Service (DoS)
- 10 Denial of Service (DoS)
- 11 Denial of Service (DoS)
- 12 Denial of Service (DoS)
- 13 Denial of Service (DoS)
- 14 Denial of Service (DoS)
- 15 Denial of Service (DoS)
- 16 Denial of Service (DoS)
- 17 Denial of Service (DoS)
- 18 Denial of Service (DoS)
- 19 Denial of Service (DoS)
- 20 Denial of Service (DoS)
- 21 Denial of Service (DoS)
- 22 Denial of Service (DoS)
- 23 Denial of Service (DoS)
- 24 Denial of Service (DoS)
- 25 Denial of Service (DoS)
- 26 Denial of Service (DoS)
- 27 Denial of Service (DoS)
- 28 Denial of Service (DoS)

Espionage

- Refers to monitoring other countries to steal secrets.

Types of industrial espionage

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

Click to add notes

Unit 1 Nishant Doshi

NOTES COMMENTS

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

CYBER WARFARE Types

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

Espionage

- Refers to monitoring other countries to steal secrets.

Type of Industrial Espionage



Sabotage

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

Sabotage (Contd.)



Click to add notes

Unit 1 Nishant Doshi

NOTES COMMENTS

24

25

26

27

28

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

CYBER WARFARE Types

- 1) Espionage
- 2) Sabotage
- 3) Denial Attack
- 4) Electrical Power Grid
- 5) Propaganda Attacks
- 6) Economic Devastation
- 7) Suicide 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 disaffected or careerless employees, or government employees with affiliation to the attacking country.

27 Sabotage (Contd.)



Click to add notes

28 Denial of Service (DoS)

Unit 1.pptx - PowerPoint

Aashka R

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

Sabotage

- Government organisations that store sensitive information and the risks if it is compromised.
- Hostile governments or terrorists may use saboteurs to carry out acts of violence under threats such as blackmail or coerce employees, or government employees with affiliation to the attacking country.

Sabotage (Contd.)

Denial of Service (DoS)

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

Denial of Service (DoS)

Diagram illustrating Denial of Service (DoS) attack:



Unit 1.pptx - PowerPoint

Aashka R -

HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Layout Reset Section Slides

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

Sabotage (Contd.)

Denial of Service (DoS)

Denial of Service (DoS)

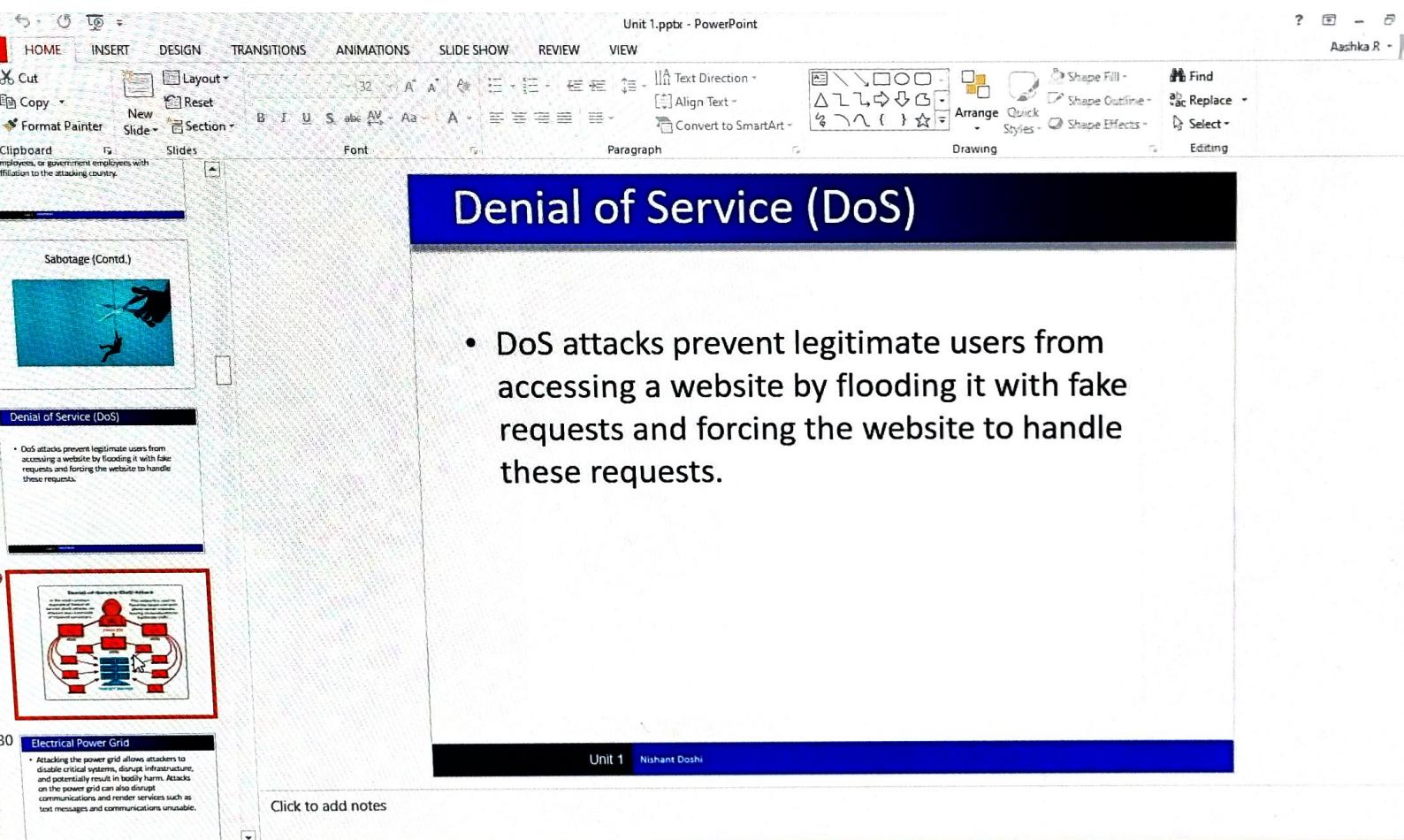
- DoS attacks prevent legitimate users from accessing a website by flooding it with fake requests and forcing the website to handle these requests.

0 Electrical Power Grid

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

Click to add notes

Unit 1 Nishant Doshi



Unit 1.pptx - PowerPoint

Aashka R.

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Layout Reset

Clipboard Slides

Font

Text Direction Align Text Convert to SmartArt

Paragraph

Text Box Shape Fill Shape Outline Quick Styles Shape Effects

Find Replace Select

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.)

32 Propaganda Attacks

Click to add notes

Unit 1 Nishant Doshi

29

30

31

32

The screenshot shows a Microsoft PowerPoint slide titled "Electrical Power Grid". The slide contains a bulleted list: "• 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." Below the slide, there are navigation icons for back, forward, and search, along with a status bar showing "Unit 1 Nishant Doshi". The left side of the screen shows a navigation pane with other slides, including one titled "Propaganda Attacks" which has a small thumbnail image of a power grid diagram.

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

Find Replace Select

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.)

32 Propaganda Attacks

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

Click to add notes

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

32 Propaganda Attacks

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

33 Propaganda Attacks (Contd.)

34 Economic Disruption

• Most modern economic systems operate using computers.

• 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.

Click to add notes

Unit 1 Nishant Doshi

NOTES COMMENTS

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste New Slide Section Slides

Clipboard

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Effects

Find Replace Select

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

Click to add notes

NOTES COMMENTS



Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste New Slide Section Layout Reset

Clipboard Slides Font Paragraph Drawing Editing

Economic Disruption

33 Propaganda Attacks (Contd.)



34 Economic Disruption

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

35 Sunrise Attacks

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

36 Cybercrime

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

Click to add notes

Unit 1 Nishant Doshi

NOTES COMMENTS

UNIT 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste Clipboard

Layout New Slide Section Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Effects

Find Replace Select

35 Sunrise Attacks

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

36 Cybercrime

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

37 Cyber Crime Case Studies

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

38 Cyber Crime Case Studies

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

Sunrise Attacks

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

Unit 1 Nishant Doshi

Click to add notes

NOTES COMMENTS

Unit 1.pptx - PowerPoint

Aashka R.

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste New Slide Section Slides Clipboard

Font Paragraph Drawing Editing

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.

Cybercrime

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

Cyber Crime Case Studies

- On 21 May 2022, it was reported that Air India was subjected to a cyberattack where the details of about 4.5 million customers around the world were compromised including passport, credit card details, birth dates, name and ticket information.

Cyber Crime Case Studies

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

Unit 1 Nishant Doshi

Click to add notes

NOTES COMMENTS

Unit 1.pptx - PowerPoint

Aashka R.

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste Clipboard Slides

Layout New Slide Section Reset

Font Paragraph

Text Direction Align Text Convert to SmartArt

Shape Fill Shape Outline Quick Styles Shape Effects

Arrange 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 experts.
- Air India also guaranteed its passengers that there was no conclusive evidence on whether any misuse of the personal data has been reported.
- The airline also urged and encouraged the passengers to immediately change their passwords.

39 Cyber Crime Case Studies

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

40 Cyber Crime Case Studies

Click to add notes

Unit 1 Nishant Doshi

NOTES COMMENTS

Unit 1.pptx - PowerPoint

Aashka R -

Cybercrime

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

Cyber Crime Case Studies

- On 21 May 2021, it was reported that Air India was hacked 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.

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.

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

Click to add notes

Unit 1 Nishant Doshi

NOTES COMMENTS

36

37

38

39

40

The screenshot shows a Microsoft PowerPoint slide titled "Cyber Crime Case Studies". The slide content includes a main section with three bullet points and four smaller sections on the left side, each with its own set of bullet points. The top navigation bar is visible, showing tabs like FILE, HOME, INSERT, DESIGN, etc., and the ribbon menu at the top.

Aashka R -

Unit 1.pptx - PowerPoint

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Clipboard Slides

Layout Reset Font Paragraph

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Fill Shape Outline Shape Effects Select Editing

Cyber Crime Case Studies

On 21 May 2021, it was reported that Air India was subjected to a cyber attack whereas the personal details of about 45 million customers around the world were compromised including passport, credit card details, birth dates, name and ticket information.

Cyber Crime Case Studies

- It was reported that the compromised details by the hackers were later acquired and Air India took steps to engage external data security specialists.
- Air India also urged passengers to change their passwords to conclude evidence on whether any misuse of the personal data has been reported.
- The airlines also urged and encouraged the passengers to immediately change their passwords.

Cyber Crime Case Studies

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

Cyber Crime Case Studies

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

Cyber Crime Case Studies

- After taking control of the administrator account via SQL injection the researcher activated his own password reset (PRCE), bypassed one-time password (OTP) authentication, and unearthed a cross-site request forgery (CSRF) bug, he claims.

Cybercrimes Classification

Click to add notes

Unit 1 Nishant Doshi

AUTHOR COMMENTS

Unit 1.pptx - PowerPoint

Aashka R

Cut Copy Format Painter Paste

Clipboard

File Insert Design Transitions Animations Slide Show Review View

Layout New Slide Section

Font

Text Direction Align Text Convert to SmartArt

Paragraph

Arrange Quick Styles Shape Effects

Drawing

Find Replace Select

Editing

Cyber Crime Case Studies

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

• 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.

• 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.

• Against individual

- Email spoofing: Email spoofing is a form of cyber attack where an attacker 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 organization to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

• Against individuals

- Spreading: Spreading is the act of messaging systems. It refers to multiple unrelated messages to large numbers of recipients for the purpose of commercial advertising, political propaganda, or harassment and pranking. In any professed purpose, or simply sending the same message to many people at once.
- Password spraying: Password spraying is an attack on the password system that is used to steal user names and passwords from the network. Many different password

Click to add notes

Unit 1 Nishant Doshi

NOTES COMMENTS

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Aashka R

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

42 Cybercrimes Classification (Contd.)

- Against Individual
 - Spamming:** Spamming is the use of messaging systems to send multiple unsolicited messages to numerous recipients for the purpose of commercial advertising, for the purpose of non-commercial promotion, or for the purpose of sending irrelevant and sending the same message over and over to the same user.
 - Password Sniffing:** Password sniffing is an attack on wireless networks that intercepts 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.)

Click to add notes

Unit 1 Nishant Doshi

NOTES COMMENTS

Cybercrimes Classification

- Against Individual
 - EMAIL Spoofing: Email spoofing is a form of cyber attack in which a hacker sends an email 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.pptx - PowerPoint

Aashka R

Cut Copy Format Painter

Layout New Slide Section Slides Font Paragraph Drawing Editing

Cybercrimes Classification (Contd.)

• Against Individual

- Email Spamming: Email spamming is a form of cyber attack in which a hacker sends an email that has been created from a stolen identity.
- 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 victims into providing sensitive data like personally identifiable information, bank and credit card details, and passwords.

• Against Individual

- Sparming: Sparming 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, or for any prohibited purpose, by sending the same message over and over to the same user.
- Password sniffing: Password sniffing is an attack on the Internet that is used to steal user names and passwords from the network. Man-in-the-middle attacks are commonly used for stealing passwords and credentials today.

• Against property:

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

• Against property:

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

Click to add notes

Unit 1 Nishant Doshi

Unit 1.pptx - PowerPoint

Aashka R -

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

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

42 Cybercrimes Classification (Contd.)

- Against individuals:
Spamming: Spamming is the use of messaging systems to send multiple unsolicited messages to large numbers of people without their consent or knowledge, for the purpose of non-commercial gain. Phishing: It is a type of social engineering attack where the attacker sends the same message over and over to the same person.

43 Cybercrimes Classification (Contd.)

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

44 Cybercrimes Classification (Contd.)

- Against property:
Intellectual property:
 - Patent infringement
 - Trademark infringement
 - Copyright infringementInternet User Theft: It refers to the theft of internet where the unauthorised person uses internet hours paid by another person.

45 Cybercrimes Classification (Contd.)

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

Click to add notes

Unit 1 Nishant Doshi

NOTES COMMENTS

85%

Cybercrimes Classification (Contd.)

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

UNIT 1-PP01 - POWERPOINT

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

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

Clipboard

Text Direction Align Text Convert to SmartArt

Find Replace Select

43 Cybercrimes Classification (Contd.)

- Against property:
 - Credit card fraud: Credit card fraud is the unauthorized use of a credit or debit card, or similar payment tool (ACH, #1), recurring charges, etc., to fraudulently obtain money or property.

44 Cybercrimes Classification (Contd.)

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

45 Cybercrimes Classification (Contd.)

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

46 Cybercrimes Classification (Contd.)

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

Unit 1 Nishant Doshi

Click to add notes

NOTES COMMENTS

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.pptx - PowerPoint

Aashka R.

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Find Replace Select

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

44 Cybercrimes Classification (Contd.)

- Against property:
 - Intellectual property:
 - Patent infringement
 - Trademark infringement
 - Copyright infringement
 - Unauthorised access: It refers to the thief in a network after the unauthorised person uses internet tools used by another person.

45 Cybercrimes Classification (Contd.)

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

46 Cybercrimes Classification (Contd.)

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

47 Indian ITA 2000

Click to add notes

Unit 1 Nishant Doshi

NOTES COMMENTS

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

C:\Users\Aashka R\OneDrive - PowerPoint

Paste Cut Copy Format Painter New Slide Section Layout Reset

Clipboard Slides Font Paragraph Drawing

Find Replace Select Editing

46 Cybercrimes Classification (Contd.)

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

47 Indian ITA 2000

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

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

(Continued)

48 Indian ITA 2000 (Contd.)

49 CYBERTERRORISM

Cyberterrorism is the premeditated, politically motivated attack against information, computer systems, computer programs and data which results in damage to, or noncombatant targets sub national groups.

Lack of information security gives rise to cybercrimes. INDIAN INFORMATION TECHNOLOGY ACT 2000 includes new focus on information security in India.

Click to add notes

Unit 1.pptx - PowerPoint

Aashka R

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 2008).

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. Like other acts of terrorism, cybercrimes, INDIAN INFORMATION TECHNOLOGY ACT 2000 provides new focus on Information security in India.

Targets

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

Click to add notes

Unit 1.pptx - PowerPoint

Aashika R +

FILE HOME DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

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

Clipboard Slides

48 Indian ITA 2000 (Contd.)

49 CYBERTERRORISM

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

50 Targets

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

51 Targets (Contd.)

```
graph TD; Root[Information System] --> Sub1[Financial Sector]; Root --> Sub2[Transportation Sector]; Root --> Sub3[Telecommunications Sector]; Root --> Sub4[Healthcare Sector]; Root --> Sub5[Manufacturing Sector]
```

Click to add notes

Unit 1 Nishant Doshi

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Paste Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Find Replace Select

Targets

- Cyberterrorism is the premeditated, politically motivated attack against information, computer systems, computer programs and data which result in violence against members of a nation, its government, or its groups.
- Lack of information security gives rise to cybercrimes. INDIAN INFORMATION TECHNOLOGY ACT (IT Act) 2000 provides new focus on Information security in India.

Targets

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

Targets (Contd.)

Cyber Terrorism Challenges

- Difficulty Identifying Attacks: 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.

Click to add notes

Unit 1 Nishant Doshi

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

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

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

Targets (Contd.)

Targets (Contd.)

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

101

102

103

104

105

106

107

108

109

110

111

112

113

114

115

116

117

118

119

120

121

122

123

124

125

126

127

128

129

130

131

132

133

134

135

136

137

138

139

140

141

142

143

144

145

146

147

148

149

150

151

152

153

154

155

156

157

158

159

160

161

162

163

164

165

166

167

168

169

170

171

172

173

174

175

176

177

178

179

180

181

182

183

184

185

186

187

188

189

190

191

192

193

194

195

196

197

198

199

200

201

202

203

204

205

206

207

208

209

210

211

212

213

214

215

216

217

218

219

220

221

222

223

224

225

226

227

228

229

230

231

232

233

234

235

236

237

238

239

240

241

242

243

244

245

246

247

248

249

250

251

252

253

254

255

256

257

258

259

260

261

262

263

264

265

266

267

268

269

270

271

272

273

274

275

276

277

278

279

280

281

282

283

284

285

286

287

288

289

290

291

292

293

294

295

296

297

298

299

300

301

302

303

304

305

306

307

308

309

310

311

312

313

314

315

316

317

318

319

320

321

322

323

324

325

326

327

328

329

330

331

332

333

334

335

336

337

338

339

340

341

342

343

344

345

346

347

348

349

350

351

352

353

354

355

356

357

358

359

360

361

362

363

364

365

366

367

368

369

370

371

372

373

374

375

376

377

378

379

380

381

382

383

384

385

386

387

388

389

390

391

392

393

394

395

396

397

398

399

400

401

402

403

404

405

406

407

408

409

410

411

412

413

414

415

416

417

418

419

420

421

422

423

424

425

426

427

428

429

430

431

432

433

434

435

436

437

438

439

440

441

442

443

444

445

446

447

448

449

450

451

452

453

454

455

456

457

458

459

460

461

462

463

464

465

466

467

468

469

470

471

472

473

474

475

476

477

478

479

480

481

482

483

484

485

486

487

488

489

490

491

492

493

494

495

496

497

498

499

500

501

502

503

504

505

506

507

508

509

510

511

512

513

514

515

516

517

518

519

520

521

522

523

524

525

526

527

528

529

530

531

532

533

534

535

536

537

538

539

540

541

542

543

544

545

546

547

548

549

550

551

552

553

554

555

556

557

558

559

560

561

562

563

564

565

566

567

568

569

570

571

572

573

574

575

576

577

578

579

580

581

582

583

584

585

586

587

588

589

590

591

592

593

594

595

596

597

598

599

600

601

602

603

604

605

606

607

608

609

610

611

612

613

614

615

616

617

618

619

620

621

622

623

624

625

626

627

628

629

630

631

632

633

634

635

636

637

638

639

640

641

642

643

644

645

646

647

648

649

650

651

652

653

654

655

656

657

658

659

660

661

662

663

664

665

666

667

668

669

670

671

672

673

674

675

676

677

678

679

680

681

682

683

684

685

686

687

688

689

690

691

692

693

694

695

696

697

698

699

700

701

702

703

704

705

706

707

708

709

710

711

712

713

714

715

716

717

718

719

720

721

722

723

724

725

726

727

728

729

730

731

732

733

734

735

736

737

738

739

740

741

742

743

744

745

746

747

748

749

750

751

752

753

754

755

756

757

758

759

760

761

762

763

764

765

766

767

768

769

770

771

772

773

774

775

776

777

778

779

780

781

782

783

784

785

786

787

788

789

790

791

792

793

794

795

796

797

798

799

800

801

802

803

804

805

806

807

808

809

810

811

812

813

814

815

816

817

818

819

820

821

822

823

824

825

826

827

828

829

830

831

832

833

834

835

836

837

838

839

840

841

842

843

844

845

846

847

848

849

850

851

852

853

854

855

856

857

858

859

860

861

862

863

864

865

866

867

868

869

870

871

872

873

874

875

876

877

878

879

880

881

882

883

884

885

886

887

888

889

890

891

892

893

894

895

896

897

898

899

900

901

902

903

904

905

906

907

908

909

910

911

912

913

914

915

916

917

918

919

920

921

922

923

924

925

926

927

928

929

930

931

932

933

934

935

936

937

938

939

940

941

942

943

944

945

946

947

948

949

950

951

952

953

954

955

956

957

958

959

960

961

962

963

964

965

966

967

968

969

970

971

972

973

974

975

976

977

978

979

980

981

982

983

984

985

986

987

988

989

990

991

992

993

994

995

996

997

998

999

1000

1001

1002

1003

1004

1005

1006

1007

1008

1009

1010

1011

1012

1013

1014

1015

1016

1017

1018

1019

1020

1021

1022

1023

1024

1025

1026

1027

1028

1029

1030

1031

1032

1033

1034

1035

1036

1037

1038

1039

1040

1041

1042

1043

1044

1045

1046

1047

1048

1049

1050

1051

1052

1053

1054

1055

1056

1057

1058

1059

1060

1061

1062

1063

1064

1065

1066

1067

1068

1069

1070

1071

1072

1073

1074

1075

1076

1077

1078

1079

1080

1081

1082

1083

1084

1085

1086

1087

1088

1089

1090

1091

1092

1093

1094

1095

1096

1097

1098

1099

1100

1101

1102

1103

1104

1105

1106

1107

1108

1109

1110

1111

1112

1113

1114

1115

1116

1117

1118

1119

1120

1121

1122

1123

1124

1125

1126

1127

1128

1129

1130

1131

1132

1133

1134

1135

1136

1137

1138

1139

1140

1141

1142

1143

1144

1145

1146

1147

1148

1149

1150

1151

1152

1153

1154

1155

1156

1157

1158

1159

1160

1161

1162

1163

1164

1165

1166

1167

1168

1169

1170

1171

1172

1173

1174

1175

1176

1177

1178

1179

1180

1181

1182

1183

1184

1185

1186

1187

1188

1189

1190

1191

1192

1193

1194

1195

1196

1197

1198

1199

1200

1201

1202

1203

1204

1205

1206

1207

1208

1209

1210

1211

1212

1213

1214

1215

1216

1217

1218

1219

1210

1211

1212

1213

1214

1215

1216

1217

1218

1219

1220

1221

1222

1223

1224

1225

1226

1227

1228

1229

1220

1221

1222

1223

1224

1225

1226

1227

1228

1229

1230

1231

1232

1233

1234

1235

1236

1237

1238

1239

1230

1231

1232

1233

1234

1235

1236

1237

1238

1239

1240

1241

1242

1243

1244

1245

1246

1247

1248

1249

1240

1241

1242

1243

1244

1245

1246

1247

1248

1249

1250

1251

1252

1253

1254

1255

1256

1257

1258

1259

1250

1251

1252

1253

1254

1255

1256

1257

1258

1259

1260

1261

1262

1263

1264

1265

1266

1267

1268

1269

1260

1261

1262

1263

1264

1265

1266

1267

1268

1269

1270

1271

1272

1273

1274

1275

1276

1277

1278

1279

1270

1271

1272

1273

1274

1275

1276

1277

1278

1279

1280

1281

1282

1283

1284

1285

1286

1287

1288

1289

1280

1281

1282

1283

1284

1285

1286

1287

1288

1289

1290

1291

1292

1293

1294

1295

1296

1297

1298

1299

1290

1291

1292

1293

1294

1295

1296

1297

1298

1299

1300

1301

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Shape Fill Shape Outline Shape Effects

Arrange Quick Styles Select

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

Targets (Contd.)

51

52

53

54

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

• 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.

• 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.

• Privacy violation.

• Secret information appropriation and data

Unit 1.pptx - PowerPoint

Aashka R

Cyber Terrorism Challenges

- Difficulty identifying attackers: It remains difficult to determine the identity of the attackers of most cyber attacks.
- Lack of boundaries: Attackers can organize from anywhere in the world and from multiple locations simultaneously.
- Speed of development: The attackers benefit the discovery of a new tool or technique and the implementation of a new tool or technique that exploits the vulnerability is getting shorter.

Cyber Terrorism Challenges

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

Cyber Terrorism Forms

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

Attack Methods

- Physical Attack:
 - Against computer facilities and/or transmission lines.
 - Accomplished by use of conventional weapons to destroy or severely injure computer and their terminal.
- Electronic Attack:
 - Use of beams 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 Nishant Doshi

NOTES COMMENTS

Unit 1.pptx - PowerPoint

Aashka R

LE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Clipboard Slides

Layout New Slide Section

Font Paragraph

Text Direction Align Text Convert to SmartArt

Shape Fill Shape Outline Quick Styles Shape Effects

Find Replace Select

Cyber Terrorism Challenges

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

Cyber Terrorism Forms

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

Attack Methods

- Physical Attack
 - Against Computer Systems: Involves destruction, damage or by use of conventional weapons to destroy or severely impair computer and their services.
 - Electromagnetic Attacks:
 - Use of power of electromagnetic energy or noise to damage or reduce the value of overhead computer security.
 - Cyber Attack
 - Use of malicious code to take advantage of software's weakness.

Cyber Terrorism Tools

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

Click to add notes

Unit 1 Nishant Doshi

Unit 1.pptx - PowerPoint

Aashka R.

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Paste Format Painter New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Find Replace Select

53 Cyber Terrorism Challenges

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

54 Cyber Terrorism Tools

- 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:

Click to add notes

Unit 1 Nishant Doshi

Unit 1.pptx - PowerPoint

Aashka R

Cyber Terrorism Tools

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

Unit 1 Nishant Doshi

Click to add notes

Clipboard Slides

Font Paragraph Drawing Editing

Find Replace Select

Text Direction Align Text Convert to SmartArt

Layout Reset Section

Cut Copy Format Painter New Slide

Home Insert Design Transitions Animations Slide Show Review View

FILE

56

57

THE 7 LAYERS OF CYBERSECURITY

Cyber Terrorism Tools

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

Attack Methods

- Physical Attack
- Electronic Attack
- Cyber Attack

Physical Attack

- Physical damage to hardware or software.
- Physical damage to hardware or software can lead to loss of data or functionality.
- Examples: Power Outage, Flood, Earthquake, Fire, etc.

Electronic Attack

- Use of power of electromagnetic energy to damage or disrupt electronic equipment.
- Examples: EMP, Cyber Attack.

Cyber Attack

- Use of malicious code to take advantage of software's vulnerabilities.

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste New Slide Section Slides

Clipboard

Physical Attack

- Agent (Trojan, Malware) or Lure (Phishing)
- Delivered by use of conventional weapons to destroy or severely injure computer and their users.

Electronic Attack

- Use of powers of electromagnetic energy or electromagnetic pulse to overload computer resources.

Cyber Attack

- Use of malicious code to take advantage of software's weaknesses.

56 Cyber Terrorism Tools

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

57 THE 7 LAYERS OF CYBERSECURITY

THE HUMAN LAYER
PERIMETER SECURITY
NETWORK SECURITY
ENDPOINT SECURITY
APPLICATION SECURITY
DATA SECURITY
MISSION CRITICAL ASSETS

Unit 1 Nishant Doshi

58

- 1: Mission Critical Assets – This is the data you need to protect.
- 2: Data Security – Data security controls protect the storage and transfer of data.
- 3: Application Security – Application security controls 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

Click to add notes

57

NOTE COMMENTS

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

CUT COPY PASTE FORMAT PAINTER NEW SECTION CLIPBOARD SLIDES

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Shape Fill Shape Outline Quick Styles Shape Effects Select

Find Replace

58

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

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

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

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

59

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

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

60

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

61

Click to add title

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

Click to add notes

Unit 1 Nishant Doshi

58

```
graph TD; A[Click to add title] --- B["• 1: Mission Critical Assets – This is the data you need to protect."]; A --- C["• 2: Data Security – Data security controls protect the storage and transfer of data."]; A --- D["• 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."]; A --- E["• 4: Endpoint Security – Endpoint security controls protect the connection between devices and the network."]; A --- F["• 5: Network Security – Network security controls protect an organization's network and prevent unauthorized access."]; A --- G["• 6: Perimeter Security – Perimeter security controls include both the physical and digital security methodologies that protect the business overall."]; A --- H["• 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."]; A --- I["Click to add notes"];
```

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Paste Format Painter Clipboard Slides

Layout New Slide Section

Font Paragraph Drawing Editing

Find Replace Select

Clipboard

58

- 1: Mission Critical Assets – This is the data you need to protect.
- 2: Data Security – Data security controls protect the storage and transfer of data.
- 3: Application Security – Application security controls protect 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 physical security 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.

Click to add notes

Unit 1 Nishant Doshi 59

NOTES COMMENTS

Diagram:

```
graph TD; A[Operational Assets] --> B[Physical]; A --> C[Financial]; A --> D[Human];
```

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste Clipboard Slides

Layout Reset Section New Slide

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Shape Fill Shape Outline Quick Styles Shape Effects

Find Replace Select

59

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

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

60

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

[No Title]

61

• Cyber Water Aktion

```
graph TD; CA[Cyber Water Aktion] --> I[Insider]; CA --> O[Outsider]; CA --> N[Non-Critical]; I --> P[Phish]; I --> M[Malware]; I --> NC[Non-Critical]
```

62

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

Click to add title

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

Click to add notes

Unit 1 Nishant Doshi 60

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section

Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Fill Shape Outline Shape Effects

Find Replace Select

Click to add title

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

1
2
3
4

62

63

64

Unit 1 Nishant Doshi

62

Click to add notes

NOTES COMMENTS

Diagram:

```
graph TD; A[Operational Areas] --> B[Voluntary]; A --> C[Voluntary]; A --> D[Voluntary]; B --> E[Political]; B --> F[Financial]; B --> G[Non-Governmental]
```

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Reset Layout

Clipboard Slides

Font Paragraph

Drawing Editing

Find Replace Select

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Effects

Click to add title

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

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

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

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

[No Title]

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

Click to add notes

Unit 1 Nishant Doshi 63

The screenshot shows a Microsoft PowerPoint presentation titled 'Unit 1.pptx'. The main slide has a blue header bar with the text 'Click to add title'. Below the header, there is a bullet point: '• deliberate actions (by insiders or outsiders) that are taken intentionally and are meant to do harm;'. In the navigation pane on the left, there are five slides numbered 52, 53, 64, [No Title], and 65. Each slide has a small preview and some text. The top ribbon menu includes FILE, HOME, INSERT, DESIGN, TRANSITIONS, ANIMATIONS, SLIDE SHOW, REVIEW, and VIEW. The HOME tab is selected. The ribbon also contains various icons for cutting, pasting, and formatting. The status bar at the bottom right shows the name 'Aashka R'.

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

Cut Copy Format Painter Paste New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

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

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

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

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

Click to add title

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

Click to add notes

Unit 1 Nishant Doshi 64

The screenshot shows a Microsoft PowerPoint slide titled "Click to add title". The slide contains a single bullet point: "• inaction (generally by insiders), such as a failure to act in a given situation, either because of a lack of appropriate skills, knowledge, guidance, or availability of the correct person to take action Of primary concern". The slide is part of a presentation with other slides visible on the left side, each containing a similar bullet point. The top ribbon shows the tabs: FILE, HOME, INSERT, DESIGN, TRANSITIONS, ANIMATIONS, SLIDE SHOW, REVIEW, and VIEW. The title bar indicates the file name is "Unit 1.pptx - PowerPoint". The status bar at the bottom right shows the name "Aashka R". The footer of the slide displays "Unit 1" and "Nishant Doshi" along with a page number "64".

Unit 1.pptx - PowerPoint

Aashka R -

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Shape Fill Shape Outline Quick Styles Shape Effects

Arrange Select

64

65

66

67

Click to add title

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

Click to add notes

Unit 1 Nishant Doshi 65

NOTES COMMENTS

The screenshot shows a Microsoft PowerPoint slide titled "Click to add title". The slide content includes a bullet point: "• **Political motivations:** examples include destroying, disrupting, or taking control of targets; espionage; and making political statements, protests, or retaliatory actions." On the left, there are thumbnails of other slides, numbered 64, 65, 66, and 67. The top ribbon shows standard options like File, Home, Insert, Design, Transitions, Animations, Slide Show, Review, and View. The Home tab is selected. The ribbon also includes font and paragraph tools, drawing tools, and a quick styles section. The status bar at the bottom right shows "Unit 1 Nishant Doshi 65".

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy New Slide Format Painter Clipboard Slides

Layout Reset Section

B I U S A AV Aa

Font Paragraph

Text Direction Align Text Convert to SmartArt

Drawing Editing

Find Replace Select

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

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.

Attacks

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

DNS Spoofing

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

Click to add notes

Unit 1 Nishant Doshi

67

Unit 1.pptx - PowerPoint

Ashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Layout Reset

Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Effects

Find Replace Select

7

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

8

Attacks

59

• Injection attack
• 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.

68

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 incorrect IP address, directing traffic to the attacker's server or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.

71

Click to add notes

Attacks

Click to add subtitle

68

FILE HOME DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste New Slide Section Slides Clipboard

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Shape Fill Shape Outline Quick Styles Shape Effects

Find Replace Select

Aashka R

67

- Socio-cultural motivations, example, 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 hardware attack in which a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attacker's computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.

71

Click to add 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

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Effects Find Replace Select

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.

70

71

72

Unit 1 Nishant Doshi

Click to add notes

NOTES COMMENTS

Unit 1.pptx - PowerPoint

Ashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Effects

Find Replace Select

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 respond with incorrect IP address of the target, to the attacker's computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.

71 ★

Session Hijacking

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

[No Title]

72 ★

Phishing

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

73 ★

Brute force

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

Click to add title

● Session Hijacking

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

Click to add notes

Unit 1 Nishant Doshi

71

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Find Replace Select

Session Hijacking

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

Phishing

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

Brute force

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

Denial of Service

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

Click to add title

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

Unit 1 Nishant Doshi

72

Click to add notes

SIDE 72 OF 96 ENGLISH (INDIA)

Type here to search

13:38 09-02-2024

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Find Replace Select

Session Hijacking

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

Phishing

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

Brute force

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

Denial of Service

- It is an attack which 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.

Click to add title

Click to add notes

Unit 1 Nishant Doshi

73

74

75

NOTES COMMENTS

Unit 1.pptx - PowerPoint

Aashka R.

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

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

Clipboard Slides

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 against the target data file or password or 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.

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 Clipboard Slides

Layout New Slide Section

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Effects

Find Replace Select

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.

5

6

76

77

75

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 Clipboard Slides

New Slide Section

Font Paragraph

Text Direction Align Text Convert to SmartArt

Drawing Editing

Find Replace Select

Clipboard

75

Dictionary attacks

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

Click to add title

• URL Interpretation

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

Click to add notes

Unit 1 Nishant Doshi

76

NOTES COMMENTS

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy New Slide Section Format Painter Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Shape Fill Shape Outline Quick Styles Shape Effects

Find Replace Select

Clipboard Slides

Dictionary attacks

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

6 URL Interpretation

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

77 File Inclusion attacks

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

78 Man in the middle attacks

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

Click to add title

Click to add notes

Unit 1 Nishant Doshi

77

Unit 1.pptx - PowerPoint

Ashka R

HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Clipboard Slides

Layout Reset New Slide Section

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Effects

Find Replace Select

JURL 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 external files which is available on the web server or to execute malicious files on the web server by making use of the include functionality.

Man in the middle attacks

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

Virus

It is a type of malicious software program that spreads throughout the computer files without the 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.

Click to add title

● **Man in the middle attacks**

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

Click to add notes

Unit 1 Nishant Doshi

78

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

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

On the left side of the Word window, there are four slide thumbnails labeled 78, 79, 80, and 81. Each thumbnail shows a list of malicious software types. The slide thumbnails are partially visible, with the first one showing 'Man in the middle attacks' and the second one showing 'Virus'.

At the bottom of the slide, there is a footer bar with the text 'Unit 1 Nishant Doshi' and a page number '79'.

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

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

On the left side of the Word window, there are four slide thumbnails labeled 79, 80, 81, and 82. Each thumbnail displays a list of malware types with some descriptive text. The status bar at the bottom right of the Word window shows the page number "80".

79 ★
• Virus
• It is a type of malicious software program that spreads 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.

Unit 1 Nishant Doshi 80

UNIT 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

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

UNIT 1.pptx - PowerPoint

80 ★

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

81 ★

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

82 ★

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

83 ★

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

Click to add title

• Trojan horse

•

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

Click to add notes

Unit 1 Nishant Doshi

81

Unit 1.pptx - PowerPoint

Aashka R.

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Effects

Find Replace Select

80

• Worm
• It is a type of malware whose primary function is to replicate itself to 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 or unusual activity, even though the user should be idle. It misleads the user of its true intent. It appears to be a normal application but when opened/executed some malicious code will run in the background.

82

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

83

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

84

Session replay: In this type of attack, a hacker

Click to add title

● **Backdoors**

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

Click to add notes

Unit 1 Nishant Doshi

82

NOTES COMMENTS

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Paste Format Painter Clipboard Slides

Font Paragraph Drawing Editing

Find Replace Select

82

Backdoors

- It is a method that bypasses the normal authentication process. A backdoor 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.**

Click to add notes

Unit 1 Nishant Doshi 83

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

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

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Shapes Quick Styles Shape Effects

Find Replace Select

83

• **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.

84

• **Bots**
A bot (short for "robot") is an automated program 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.

85

• **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.

86

• **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

● **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.

Click to add notes

Unit 1 Nishant Doshi 84

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Shape Fill Shape Outline Quick Styles Shape Effects

Find Replace Select

84

Session number in this type of attack is known as an **spoofed session**. 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

In a **distributed denial of service (DDoS)** exploit, large numbers of compromised systems (botnet) send requests to a single target.

86

In a **denial of service (DoS)** attack, the attacker sends a large number of requests to a target system, causing it to respond slowly or stop responding. This may be recovered by the user.

Click to add title

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

Unit 1 Nishant Doshi

85

Click to add notes

SLIDE 85 OF 96 ENGLISH (INDIA)

Type here to search

13:38 09.02.2024

Unit 1.pptx - PowerPoint

Aashka R.

HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter

New Slide Section

Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Effects

Find Replace Select

Click to add title

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

7

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

7 ★ • Coverdropping (Fragging): the attacker simply listens to messages exchanged by two hosts. For the attack to succeed, the message must not be encrypted. An unencrypted message, such as a password sent in response to an HTTP request, may be retrieved by the attacker.

88

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

Click to add notes

Unit 1 Nishant Doshi 86

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Paste Format Painter New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Shape Fill Shape Outline Quick Styles Shape Effects

Find Replace Select

Click to add title

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

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

88 • **Traffic analysis**: the attacker looks at the metadata transmitted in traffic in order to deduce information relating to the exchange and the participating entities, e.g. the form of the exchanged traffic (rate, duration, etc.). In the 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 notes

Unit 1 Nishant Doshi

87

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Effects Select

87

- **Covert channels (hopping)**: the attacker simply listens to messages exchanged by two entities. For the attack to be useful, the traffic must not be encrypted. If encrypted communication, 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

- **Need of Security policies**
 - 1. It increases efficiency and accountability
 - 2. It can enable or disable a function that
 - 3. Helps in reducing complexity in security filtering

Click to add title

Click to add notes

Unit 1 Nishant Doshi

88

NOTES COMMENTS

SLIDE 88 OF 96 ENGLISH (INDIA) Type here to search 13:39 09-02-2024 35%

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

- **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.

The slide has a blue header bar with the title and a dark blue footer bar with navigation links. The left sidebar lists slide numbers 87, 88, 89, and 90, each with a small preview image. The bottom taskbar shows the Windows Start button, a search bar, and various pinned application icons.

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Layout Reset

Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Effects

Find Replace Select

Click to add title

7

• **Man-in-the-middle (MitM)**: 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.

8

• **Traffic analysis**: the attacker looks at the metadata transmitted in traffic in order to deduce information about the communication between 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

• 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

Click to add notes

Unit 1 Nishant Doshi 89

Unit 1.pptx - PowerPoint

Aashka R

FILE INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

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

39

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

40

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

91

• Virus and Spyware Protection policy:
- It helps to detect threats in files, in default applications and enables suspicious behavior.
- Removes, and repairs the side effects of viruses and removes 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 intrusion of network traffic.

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

Aashka R

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.

89

★

- Software Malware: 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

★

92

★

- 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.

93

91

Unit 1 Nishant Doshi

Click to add notes

NOTES COMMENTS

Unit 1.pptx - PowerPoint

Aashka R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

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

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Shapes Quick Styles Shape Effects

Find Replace Select

90 ★ Need of Security policies:

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

91 ★ Virus and Spyware Protection policy:

- It helps to detect threats in files, to delete applications that exhibits suspicious behavior.
- Removes, and removes 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.

Click to add notes

Unit 1 Nishant Doshi

92

Aashika R

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter Paste New Slide Section Clipboard

It can make or break a business deal
It helps to educate employees on security literacy

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Shapes Quick Styles Shape Effects

Find Replace Select

91

Virus and Spyware Protection policy:

- It finds to detect threats in files, to detect applications that exhibits suspicious behavior.
- Removes, and removes the side effects of viruses and removes risks by using signatures.

92

Firewall Policy:

- Blocks the unauthorized users from accessing the systems and restricts the access 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 application 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

Aashka R.

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

Cut Copy Format Painter New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Shapes Quick Styles Shape Effects

Find Replace Select

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.

93

+ Intrusion Prevention policy:

- This policy automatically detects and blocks the network attacks and browser threats.
- It also prevents 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.

95

References

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

96

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 Paste Format Painter New Slide Section Clipboard Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Shape Fill Shape Outline Quick Styles Shape Effects

Find Replace Select

Intrusion Prevention policy:

- This policy automatically detects and blocks the network attacks and botnet attacks.
- It also prevents applications from vulnerability and checks the existence of new or old data file keys and corrects it where attack is coming through legal ways.

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 controls are applied to both Windows and Mac computers whereas application control policies can be applied only to Windows clients.

References

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

95 References

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

96 Click to add notes

Unit 1 Nishant Doshi

NOTES COMMENTS

3

4

94

95

96

Unit 1.pptx - PowerPoint

Aashka R -

FILE HOME INSERT DESIGN TRANSITIONS ANIMATIONS SLIDE SHOW REVIEW VIEW

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

Clipboard Slides

Font Paragraph Drawing Editing

Find Replace Select

93 * Intrusion Prevention policy:

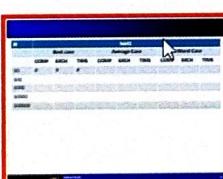
- This policy automatically detects and blocks the attacks to a system and can detect them.
- It also protects applications from vulnerabilities and checks the contents of one or more data packages and detects malware which is entering through legal ways.

94 * Application and Device Control:

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

95 * References:

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

96 * 

Click to add title

Sort1

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

Unit 1 Nishant Doshi 96

Click to add notes