Information Security

Introduction to Information Security

What is InfoSec?

Most expensive assets in the world are digital
Every field with digital information requires Security.

Information security encompasses safeguarding data from unauthorized access, disclosure, alteration, or

destruction. Who can do a Data Breach

- An Accidental Insider
- A Malicious Insider
- Lost or Stolen Devices
- Malicious Outside Criminals

Need For Cybersecurity

The CIA Triad

Confidentiality

Confidentiality is about preventing the disclosure of data to unauthorized parties.

Integrity

Integrity refers to protecting information from being modified by unauthorized parties.

Availability

Availability is making sure that authorized parties are able to access the information when needed

Confidentiality

Integrity

Availab

Attacks

- Cracking Encrypted Data
- Man In The Middle
- Installing Spyware
- Doxxing

- Web Penetration
- Unauthorised Scans
- Remote Controlling

- DDoS attacks
- Ransomware Attacks
- Disrupting Se

Countermeasures

- Access Control
- Encryption
- Biometric Verification

- Intrusion Detection
- Cryptography
- Hashing

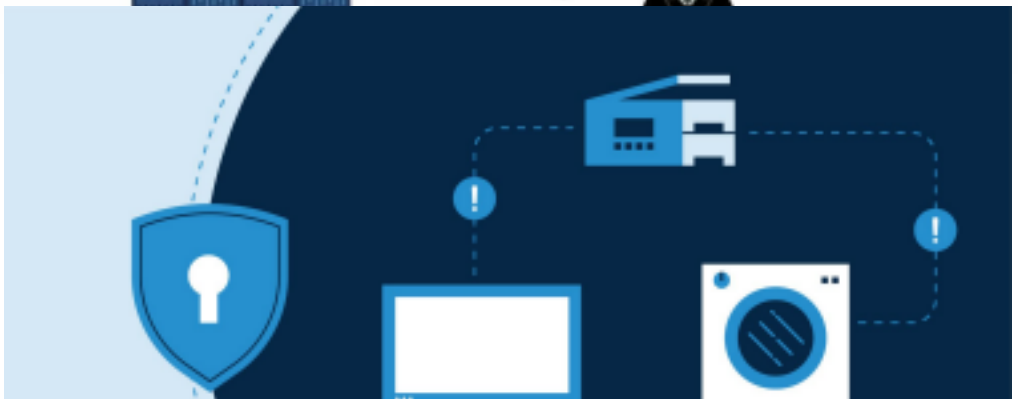
- Regular Backu
- Data Replicati
- Adequate com bandwidth

Types of Security

Network Security

Network security focuses on protecting data transmitted over networks from unauthorized access, modification, or interception.

IoT Security



Protect Internet of Things (IoT) devices, networks,

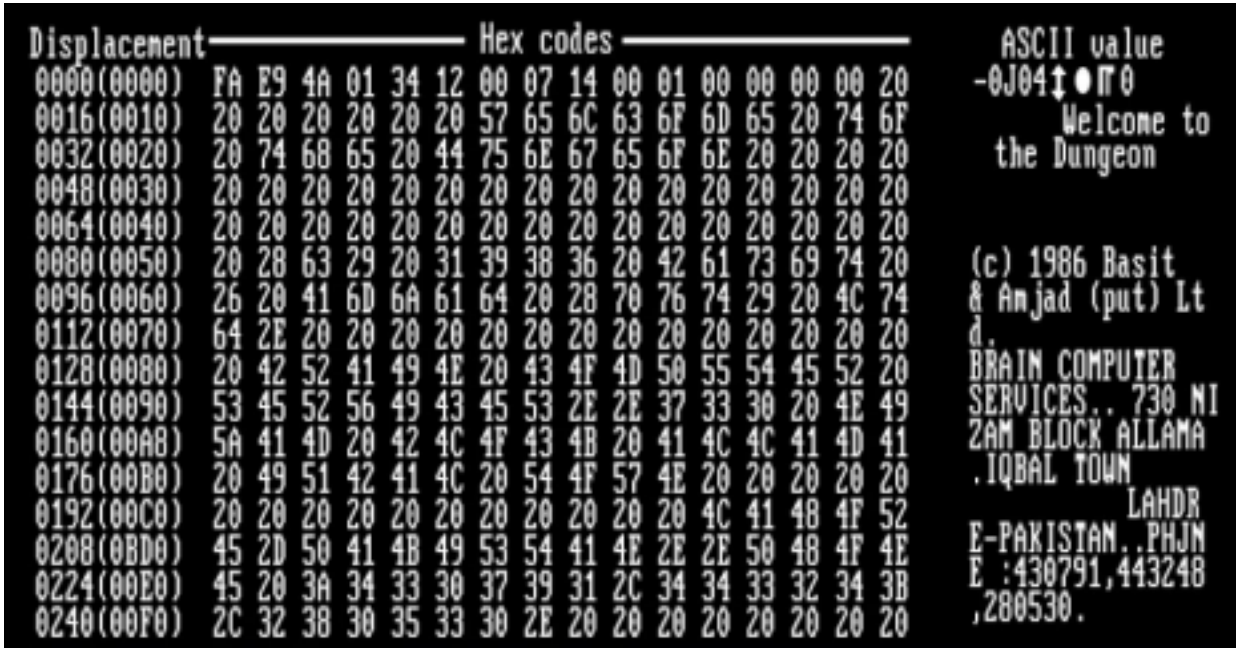
and data from threats.

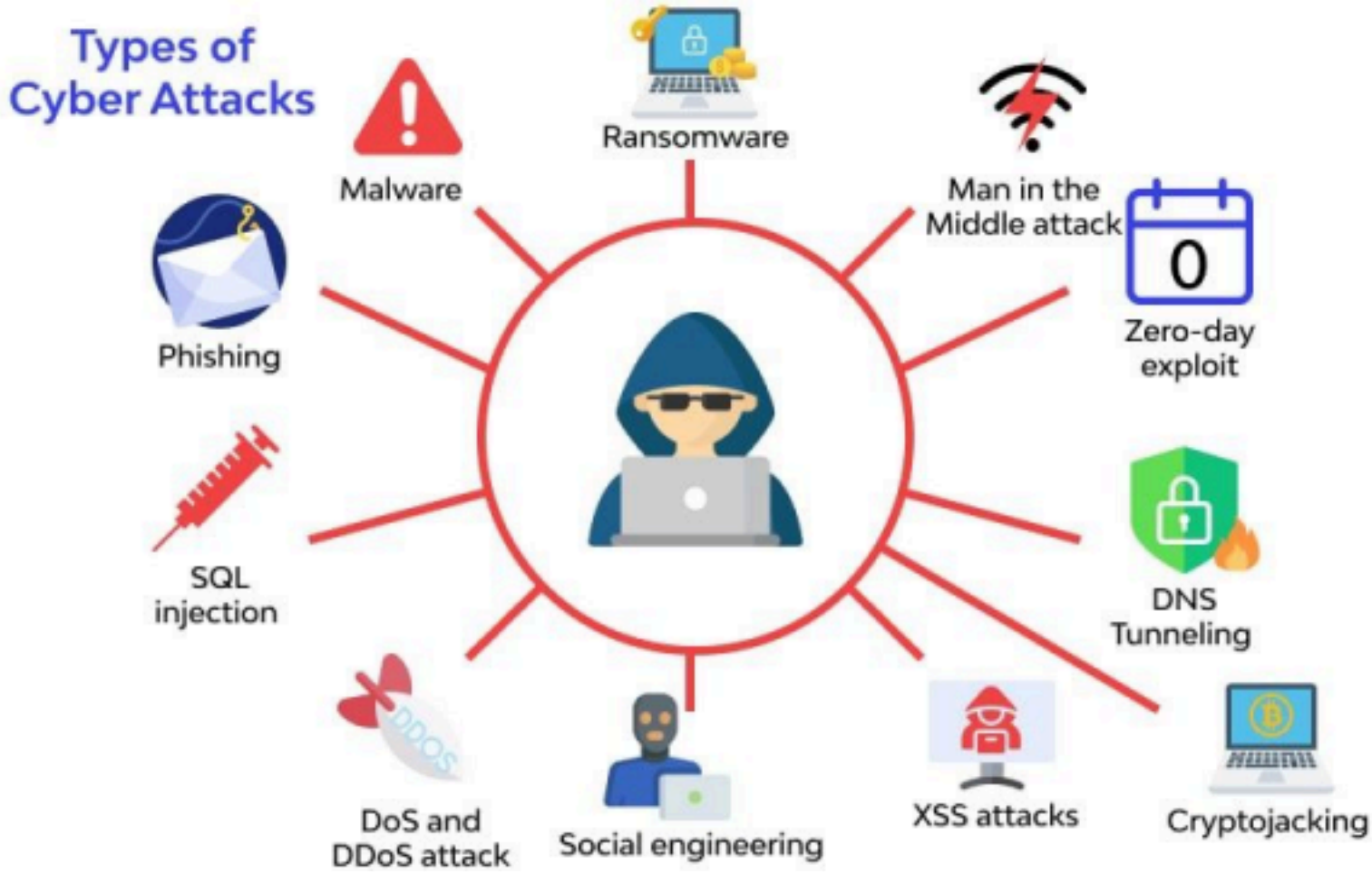
AI Security

Protection of AI systems and

infrastructure from latest attacks.

What is a cyber attack?


Displacement Hex codes ASCII value
0000(0000) FA E9 4A 01 34 12 00 07 14 00 01 00 00 00 00 20 -0J04↕●╥0
0016(0010) 20 20 20 20 20 20 57 65 6C 63 6F 6D 65 20 74 6F Welcome to
0032(0020) 20 74 68 65 20 44 75 6E 67 65 6F 6E 20 20 20 20 the Dungeon
0048(0030) 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0064(0040) 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0080(0050) 20 28 63 29 20 31 39 38 36 20 42 61 73 69 74 20 (c) 1986 Basit
0096(0060) 26 20 41 6D 6A 61 64 20 28 70 76 74 29 20 4C 74 & Amjad (put) Lt
0112(0070) 64 2E 20 20 20 20 20 20 20 20 20 20 20 20 20 20 d.
0128(0080) 20 42 52 41 49 4E 20 43 4F 4D 50 55 54 45 52 20 BRAIN COMPUTER
0144(0090) 53 45 52 56 49 43 45 53 2E 2E 37 33 30 20 4E 49 SERVICES.. 730 NI
0160(00A8) 5A 41 4D 20 42 4C 4F 43 4B 20 41 4C 4C 41 4D 41 ZAM BLOCK ALLAMA
0176(00B0) 20 49 51 42 41 4C 20 54 4F 57 4E 20 20 20 20 20 .IQBAL TOWN
0192(00C0) 20 20 20 20 20 20 20 20 20 20 20 20 4C 41 48 4F LAHDR
0208(0BD0) 45 2D 50 41 4B 49 53 54 41 4E 2E 2E 50 48 4F 4E E-PAKISTAN..PHJN
0224(00E0) 45 20 3A 34 33 30 37 39 31 2C 34 34 33 32 34 3B E :430791,443248
0240(00F0) 2C 32 38 30 35 33 30 2E 20 20 20 20 20 20 20 20 ,280530.


Types of Cyber Attacks
Malware
Ransomware
Man in the Middle attack
Phishing
0
Zero-day exploit
SQL injection
DNS Tunneling
DDOS
DoS and DDoS attack
Social engineering
XSS attacks
Cryptojacking

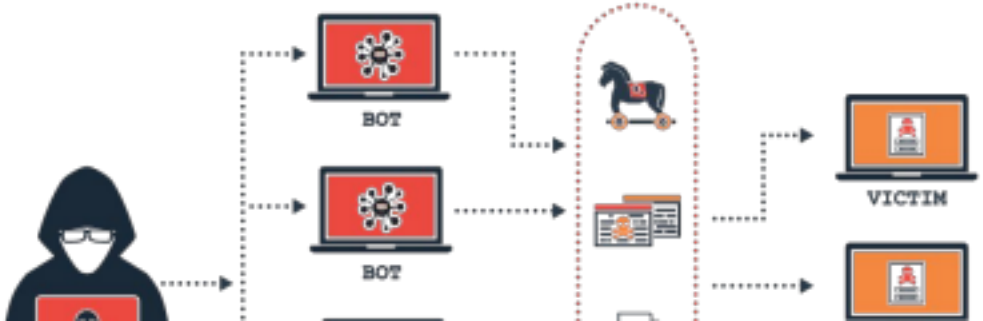
Phishing Attack

You receive an email pretending to be from your bank, asking you to click a link and update your account details. The link leads to a fake website that steals your login credentials.

The "Google Docs Phishing Attack" in 2017 was particularly attention-grabbing. Attackers sent out emails with the subject "Open in Docs" or something similar. However, the page was a well-crafted phishing site.

Denial of Service (DoS) Attack

Mirai (2016) was a DoS that turns networked devices running Linux into remotely controlled bots that can be used as part of a botnet in large-scale network attacks. It



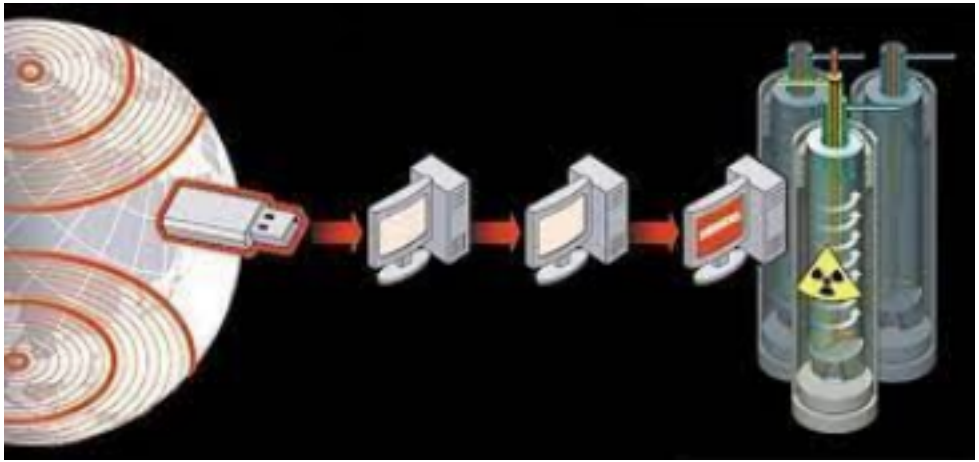
primarily targets online consumer devices such as IP cameras and home routers.

What is Distributed Denial of Service? (DDoS attack)

Malware (Malicious Software)

You download a seemingly harmless attachment that contains a virus. Once opened, it infects your computer and steals your personal files or does other harmful actions.

Stuxnet example…



There are even more…

1. Distributed Denial of Service (DDoS) Attack 2.
Ransomware Attack
3. Man-in-the-Middle (MitM) Attack 4.
SQL Injection
5. Zero-Day Exploit
6. Brute Force Attack
7. Advanced Persistent Threat (APT)

Capture The Flag (CTF) activity

https://overthewire.org/wargames/bandit

Exploration Assignment-1

1. Vulnerability
2. Exploitation

3. Debugging (GDB Installation)
4. White, Grey and Black Hat Hackers
5. Shell Code Execution
6. Firewall
7. SSL
8. VPN
9. Tcpdump (Wireshark Installation)
10. Installation of Ubuntu VM in your laptops
11. CTF Activity

Quiz in next class

Textbook and reference material

● Cryptography and Network Security: Principles and Practice by William Stallings ● Computer_Security_Principles_and_Practice_(3rd_Edition) by William Stallings

And if you want to go extra mile …

● Hacking: The Art of Exploitation, 2nd Edition by Jon Erickson
● Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software ●

Marks Distribution

Assignments, Quizzes, Project and Papers

For submissions and queries: huzaifa.nazir@pucit.edu.pk

Laptops and internet required in every class