BMS Institute of Technology and Management

(An Autonomous Institution, Affiliated to VTU, Belagavi)

Department of MCA

Cyber Security – 22MCA3053 Question Bank Module Wise.

MODULE-I Introduction to Cybercrime & Security

Course Coordinator: Dr. Shivakumara T, Assistant Professor, Department of MCA, BMSITM

CO1	Explore the Cyber Security Principles.
CO2	Apply the cyber security concepts to secure from cyber-attacks.
CO3	Formulate the possibilities of cyber-attacks in a given usecase, as a penetration tester.
CO4	Analyze cyber security tools to protect individual data.
CO5	Apply Digital Forensic tools to address cyber security issues.

Q1) Justify your views on the need of cyber security measures to be taken against the protection of assets.

Q2) With an example, define the following

a. Cyber Security
b. Cyber space
c. Cyber Squatting
d. Email Spoofing
e. Spamming
f. Cyber Defamation
g. Internet Time Theft
h. Salami Attack
i. Data diddling
j. Forgery
k. Web Jacking
l. Industrial spying / Industrial espionage
m. Hacking
n. Online frauds
o. Pornographic offenses
p. Software Piracy
q. Compute Sabotage
r. E-mail bombing / Mail Bombs

s. Usenet Newsgroup
t. Password sniffing
u. Social Engineering
v. Shoulder Surfing
w. Dumpster Diving
x. Fake S
y. Baiting
z. Cyberstalking
aa. Attack vector
bb. A Zero Day Attack

Q3) Who are cyber criminals? Which are the type of attacks of cybercrime.

Q4) Which are the frequent electronic devices used for cyber-criminal activities.

Q5) Discuss the cybercriminal categories with a suitable example each.

Q6) Discuss the all 5 classification of cybercrimes.

Q7) Explain step by step how cybercriminals plan the attack?

Q8) Which are the type of cyber-attacks?

Q9) What do you understand the Reconnaissance phase of cyber-attack?

Q10) What are the differences between active attack and passive attack?

Q11) Name any 5 tools used for active attack?

Q12) Name any 5 tools used for passive attack?

Q13) What are the objectives of the Scanning in the cyberattacks?

Q14) Which are the information is revealed by PORT Scanning during cyberattacks?

Q15) Which are the information is revealed by NETWORK Scanning during cyberattacks?

Q16) Which are the information is revealed by VULNERABILITY Scanning during cyberattacks?

Q17) Discuss the Cyber Security Principles / Triad with a suitable example?

Q18) What do you understand the enumeration in the scrutinizing phase of cyberattack?

Q19) Write the differences between Offensive and Defensive Cyber Security?

Q20) Discuss the illegal activities observed in cybercafes'.

Q21) Justify your views on Botnets "the fuel of cybercrime".

Q22) Which are the primary tools to block the attack vectors?

Q23) Discuss the different ways to launch attack vectors?

Q24) Define offensive cyber security?

Q25) Discuss Tools and methods used for offensive security?

Q26) Define defensive cyber security?

Q27) Discuss Tools and methods used for defensive security?

Q28) Apply criminal attacks phases to steal information about individual identity?

Q29) Which are the precautions needs to be taken as a victim of the attack? Discuss your views.

Q30) Explain the social Engineering Life cycle with the suitable case of cybercrime.

Q31) Discuss the social engineering life cycle.

Q32) Discuss the classification of social engineering cybercrime and illustrate any two types.

Q33) Case study

Scenario-1:

An employee, unhappy with his current employer, decides to copy company information consisting of client files and confidential product information onto an external USB hard drive. After he steals the information, he proceeds to delete folders from the company server. A few months after leaving his company, the former employee starts his own business using the stolen information.

Follow the Forensic Investing Strategic Planning

Case in Point United States of America v. Biswamohan Pani, 2008 Biswamohan Pani was an employee at Intel. While working for Intel, he gave a resignation notice and while on leave from Intel, obtained a job at AMD, a competing manufacturer of computer chips. Having access to both AMD and Intel at the same time, Pani copied electronic files from Intel to an external hard drive. Pani's intention was to use the stolen files to benefit his new position at AMD.

Investigative tips: Intellectual property theft by employees is a serious threat to any business. The security of information by an organization requires that employees are able to access the information needed to perform their duties, while at the same time, the employer has no option but to trust that the information will not be stolen. Nondisclosure agreements, employment agreements, and promises do not prevent the theft of intellectual property as it only helps litigate the damage afterward. If a suspect has not already been caught with stolen intellectual property, the first course of action is to determine what data has been stolen, when it was stolen, and which persons had access during those times. Many large or high-tech companies secure confidential data through a series of safeguards. One safeguard could be allowing the fewest persons necessary to have access to the data. Another safeguard is requiring a series of secure logins to access the data, with every login recorded with as much detail as possible.

Q34) Write the importance of Reconnaissance phase of cyber-attack?

NOTE: ALWAYS GO WITH TEXTBOOKS AND REFERENCE BOOKS TO EXPLORE MORE PROBABLE QUESTIONS.

----------xxxxx----------xxxxx----------xxxxxx----------xxxx-----

MODULE-II - Introduction to Tools and Methods used in Cybercrime

Q1) In detail explain the cybersecurity hygiene.

Q2) Why, cybersecurity hygiene very much important to the current scenario of information technology?

Q3) Explain the different classification of basics tools of cyber security?

Q4) Why is finding insider threat so difficult?

Q5) Consider the context of Educational Institution.

i. Identify and write the appropriate tools to continuously monitoring day to day activities.
ii. If cyber-attacks happen, what is your defensive steps to protect the Institution.

Create the report of attack life cycle.

Q6) Consider the context of Bank Scenario.

i. Identify and write the probable vulnerabilities
ii. Identify the Threat possibilities
iii. Suggest remedial action about the vulnerabilities and threats.

Q7) Write the differences between packet filter versus firewalls.

Q8) List the general security attacks.

Q9) How an attacker can compromise a network?

Q10) What is proxy server? What are the uses of proxy server?

Q11) What is anonymizer?

Q12) What is the difference between proxy servers and anonymizers?

Q13) Elaborate, your understanding on framing strong passwords?

Q14) List the password attack types?

Q15) Explain all the password attack types in details with a suitable example.

Q16) Name any 5 important password cracking tools.

Q17) Which are the factors are considered during password cracking?

Q18) Write name of the tools required to assess threat, vulnerability and impact?

Q19) What do you understand about penetration testing in cyber security?

Q20) Which are the most common penetration testing types supported, Explain?

Q21) Write and list any 5 best pen testing tools used in the market?

Source: https://www.peerspot.com/articles/9-soar-use-cases-for-cybersecurity

NOTE: ALWAYS GO WITH TEXTBOOKS AND REFERENCE BOOKS TO EXPLORE MORE PROBABLE QUESTIONS

MODULE-III NETWORK MONITORING TOOLS (IN Progress)

Q1) Justify your views, how virtual private networks are safe for communication.

Q2) Write the differences between packet filter versus firewalls.

Q3) With a suitable scenario, Explain Network Address Translation.

Q4) What is a Firewall? Explain the different types of firewalls in detail.

Q5) What are all the uses of security frameworks. Which are framework is most widely used in India?

Q6) With a suitable scenario, Explain Network Address Translation.

Q7) What is the importance of threat analysis phase in vulnerability assessment?

Q8) Write the importance of the tools used in Social Engineering

Q9) What do you understand the Network Monitoring Tools.

Q10) Write the differences between red team and blue team in network monitoring tools

Q11) What is network detection and response?

Q12) When an adversary happens in the organization network, what are the precaution measures needs to be taken from blue security team. Explain each steps with suitable example.

Q13) Which are five techniques among the most commonly used social engineering attacks?

Q14) How to prevent social engineering attacks? Justify your views.

Q15) List out the biggest mistakes a user usually does in network security?

Q16) What do you understand about intrusion prevention systems?

Q17) How a firewall protects a network, explain with suitable example.

Q18) Explain spoofing with a suitable example.

Q19) Explain anti spoofing with a suitable example

Q20) Write the difference between stateless versus stateful firewalls.

MODULE-IV (IN Progress)

Topics

Introduction to intrusion, Physical theft
Abuse of Privileges
Baiting, external **reconnaissance**
Intrusion detection techniques
Intrusion prevention techniques
Network-based Intrusion
Detection Systems
Host-Based Intrusion Prevention Systems.

Q1) What is an intrusion detection system (IDS)? Explain the steps involved in IDS and also explain the drawbacks of IDS.

Q2) What do you understand the abuse of privileges? How can we prevent physical theft in cyber security?

Q3) What are the techniques used for intrusion detection and prevention?

Q4) What are the types of network intrusion detection systems?

Q5) What kind of attack type is baiting?

Q6) Write note on external reconnaissance

Q7) Define host based intrusion prevention systems.

Q8) What is the importance of IDS, IPS, HBIPS in cyber security

MODULE-V (IN Progress)

Topics

Audit, Authentication, Biometrics

Scanning and Threat management

Cryptography and Security policy

cyber forensics and digital evidence, forensic analysis of E-mail

Digital Forensics Process, Phases in Computer Forensics / Digital Forensics,

The security / Privacy Threats

Understanding the types of Cellular Networks, Handheld devices and Digital Forensics

IPR, TradeMarks, Copyright, Patent and Cyber Laws,

Q1) Which are the ten cyber security safeguards to be followed to protect our organizational network.

Q2) What are the 4 types of access controls? Explain any two.

Q3) What do you understand about identity theft? Explain the types of Identity theft.

Q4) With neat diagram, explain the forensics lifecycle process in detail?