Shivaji University , Kolhapur
Question Bank For Mar 2022 (Summer) Examination

Subject Code: 81551 Subject Name: Cyber Security

Question Bank Set-1

Sr No	Multiple choice questions
a	Which of the following are firewall configurations? A. Network host based B. Dual homed host C. Screened host D. All of the above
b	Which of the following is not a type of cybercrime? A. Data theft B. Forgery C. Damage to data and systems D. Installing antivirus for protection
c	Which of the following is independent malicious program that need not host program? A. Trapdoors B. Trojan horse C. Virus D. Worm
d	Which layer of the OSI model is divided into two sub layers? A. Data link B. Network C. Presentation D. Session
e	What is the basic mechanism behind a DoS attack? A. Computers don’t handle TCP packets well. B. Computers can only handle a finite load. C. Computers cannot handle large volumes of TCP traffic. D. Computers cannot handle large loads
f	What is the primary way a virus scanner works? A. By comparing files against a list of known virus profiles B. By blocking files that copy themselves C. By blocking all unknown files D. By looking at files for virus-like behavior
g	When IT Act 2000 came into effect? A. October 17, 2000 B. October 17, 2001 C. November 11, 2000 D. November 11, 2001

h	What is spyware? A. Any software that monitors your system B. Only software that logs keystrokes C. Any software used to gather intelligence D. Only software that monitors what websites you visit
i	What are the three approaches to security? A. Perimeter, layered, hybrid B. High security, medium security, low security C. Internal, external, and hybrid D. Perimeter, complete, none
j	What is SPI? A. Stateful packet inspection B. System packet inspection C. Stateful packet interception D. System packet interception
k	Blocking incoming ICMP packets will prevent what type of scan? A. SYN B. Ping C. FIN D. Stealth
l	How can securing internal routers help protect against DOS attacks? A. Attacks cannot occur if your internal router is secured. B. Because attacks originate outside your network, securing internal routers cannot help protect you against DoS. C. Securing the router will only stop router-based DoS attacks. D. It will prevent an attack from propagating across network segments
m	If a class B network on the Internet has a subnet mask of 255.255.248.0, what is the maximum number of hosts per subnet? A.1022 B.1023 C.2046 D.2047
n	A seller bidding on her own item to drive up the price is referred to as what? A. Bid siphoning B. Bid shielding C. Shill bidding D. Ghost bidding
2.	**Solve the following questions**
a	Explain SQL Script Injection with example
b	Explain concept of Cyber Stalking in detail with example

c	Explain various types of threats?
3.	**Solve the following questions**
a	What is Penetration Testing? Explain step by step process and methods
b	How to detect and eliminate virus, spyware. Explain in detail
c	What is Dos? Illustrate with example
4	**Solve the following questions**
a.	How to configure the firewall?
b	What is digital signature? How it works
c	Elaborate Intrusion-Detection system in detail?
5	**Solve the following questions**
a	Explain various cyber security standards?
b	Explain different types of operating system utilities?
c	Explain procedure for getting back deleted files?

Shivaji University , Kolhapur
Question Bank For Mar 2022 (Summer) Examination

Subject Code: 81551 Subject Name: Cyber Security

Question Bank Set-2

Sr. No	Multiple choice questions
a	Which of the following is an objective of network security? a) Confidentiality b) Integrity c) Availability d) All of the above
b	Who is the father of computer security? a) August Kirchhoff's b) Bob Thomas c) Robert d) Charles
c	What does cyber security protect? a) Cyber security protects criminals b) Cyber security protects internet-connected systems c) Cyber security protects hackers d) None of the mentioned
d	What is Cyber Security? a) Cyber Security provides security against malware b) Cyber Security provides security against cyber-terrorists c) Cyber Security protects a system from cyber-attacks d) All of the mentioned
e	Which of the following is the hacking approach where cyber-criminals design fake websites or pages for tricking or gaining additional traffic? a) Pharming b) Website-Duplication c) Mimicking d) Spamming
f	What is the existence of weakness in a system or network is known as? a) Attack b) Exploit c) Vulnerability d) Threat
g	Which of the following is an internet scam done by cyber-criminals where the user is convinced digitally to provide confidential information. a) MiTM attack b) Phishing attack c) Website attack d) DoS attack

h	Which of the following term refers to a group of hackers who are both white and black hat? a) Yellow Hat hackers b) Grey Hat hackers c) Red Hat Hackers d) White-Black Hat Hackers
i	A computer ________ is a malicious code which self-replicates by copying itself to other programs. a) program b) virus c) application d) worm
j	____________ is data-link layer vulnerability where stations are forced to make direct communication with another station by evading logical controls. a) VLAN attack b) VLAN Circumvention c) VLAN compromisation method d) Data-link evading
k	Which of the following is an example of physical layer vulnerability? a) MAC Address Spoofing b) Physical Theft of Data c) Route spoofing d) Weak or non-existent authentication
l	According to the CIA Triad, which of the below-mentioned element is not considered in the triad? a) Confidentiality b) Integrity c) Authenticity d) Availability
m	Data ___________ is used to ensure confidentiality. a) Encryption b) Locking c) Deleting d) Backup
n	Data integrity gets compromised when _____ and _____ are taken control off. a) Access control, file deletion b) Network, file permission c) Access control, file permission d) Network, system
2.	**Solve the following questions**
a	Explain the following terms related to Cyber Security a) Hacker Slang b) Script Kiddies c) Phreaking

b	Define Protocol? Explain Purposes of Different TCP/IP Protocols?
c	Explain the following 1) FakeAV 2) MacDefender 3) The Mimail Virus 4) The Bagle Virus
3.	**Solve the following questions**
a	Explain How can you Protect Against Investment Fraud and Identity Theft?
b	Explain Different Windows Hacking Techniques?
c	Explain Passive and Active Scanning Technique?
4	**Solve the following questions**
a.	What is Authentication? Explain Different Authentication protocols?
b	Explain the following 1) Snort 2) Honeypot 3) Intrusion Deterrence 4) Intrusion Deflection
c	Explain roles of international laws?
5	**Solve the following questions**
a	Explain the objectives of IT Act**?**
b	Describe the different operating system utilities that can be useful in gathering forensic data.
c	Explain the FBI Forensics Guidelines?

Shivaji University, Kolhapur

Question Bank For Mar 2022 (Summer) Examination

Subject Code: 81551 Subject Name: Cyber Security

Question Bank Set-4

Sr. No	Multiple choice questions
a	In a computer forensics investigation, what describes the route that evidence takes from the time you find it until the case is closed or goes to court? A. Rules of evidence B. Law of probability C. Chain of custody D. Policy of separation
b	Where does Linux store email server logs? A. /var/log/mail.* B. /etc/log/mail.* C. /mail/log/mail.* D. /server/log/mail.*
c	What is the term for a fake system designed to lure intruders? A. Honey pot B. Faux system C. Deflection system D. Entrapment
d	What method do most IDS software implementations use? A. Anomaly detection B. Preemptive blocking C. Intrusion deterrence D. Infiltration

e	How do most antispyware packages work? A. By using heuristic methods B. By looking for known spyware C. The same way antivirus scanners work D. By seeking out TSR cookies
f	Which of the following is not a valid IP address? A. 127.0.0.1 B. 295.253.254.01 C. 127.256.5.2 D. 245.200.11.1
g	What was most interesting to security experts about the Mimail virus? A. It spread more rapidly than other virus attacks. B. It spread in multiple ways. C. It grabbed email addresses from documents on the hard drive. D. It deleted critical system files
h	When plain text is converted to unreadable format, it is termed as ______________ a) rotten text b) raw text c) cipher-text d) cipher-text
i	______________ buffer overflows, which are more common among attackers. a) Memory-based b) Queue-based c) Stack-based d) Heap-based
j	__________________ is the kind of firewall is connected between the device and the network connecting to internet. a) Hardware Firewall b) Software Firewall c) Stateful Inspection Firewall d) Microsoft Firewall

k	Packet filtering firewalls are deployed on ________ a) routers b) switches c) hubs d) repeaters
l	ACL stands for _____________ a) Access Condition List b) Anti-Control List c) Access Control Logs d) Access Control List
m	Which of these comes under the advantage of Circuit-level gateway firewalls? a) They maintain anonymity and also inexpensive b) They are light-weight c) They're expensive yet efficient d) They preserve IP address privacy yet expensive
n	____________ works in background and steals sensitive data. a) Virus b) Shareware c) Trojan d) Adware
2.	**Solve the following questions**
a	Explain how internet fraud works?
b	Explain perimeter and layered security approach?
c	What is federal trade commission and auction fraud?
3.	**Solve the following questions**
a	Explain DDos with example?
b	Write a note on 1)W32/Netsky-F 2)Troj/Invo-zip
c	What is TCP SYN flood attack? Explain in detail
4	**Solve the following questions**
a.	What is firewall? Explain types of firewalls

b	Write a note on 1)Snort 2)Honey Pots
c	Explain the following 1)Subscriber Identity Module 2) International Mobile Subscriber Identity 3) Integrated Circuit Card Identification 4) International Mobile Equipment Identity
5	**Solve the following questions**
a	What is digital signature? How it works?
b	Explain different tools used for conducting forensic analysis and examination
c	Explain the Indian cyberspace?

Shivaji University , Kolhapur
Question Bank For Mar 2022 (Summer) Examination

Subject Code: 81551 Subject Name: Cyber Security

Question Bank Set-5

Sr. No	Multiple choice questions
a	Which of the following are important to the investigator regarding logging? A. The logging methods B. Log retention C. Location of stored logs
b	In a computer forensics investigation, what describes the route that evidence takes from the time you find it until the case is closed or goes to court? A. Rules of evidence B. Law of probability C. Chain of custody D. Policy of separation
c	Which of the following is the most common way for a virus scanner to recognize a virus? A. To compare a file to known virus attributes B. To use complex rules to look for virus-like behavior C. To only look for TSR programs D. To look for TSR programs or programs that alter the Registry
d	Which of the following is a vulnerability scanner specifically for Windows systems?

	A. Nmap B. OphCrack C. Nessus D. MBSA
e	What do you call a DoS launched from several machines simultaneously? A. Wide-area attack B. Smurf attack C. SYN flood D. DDoS attack
f	A seller bidding on her own item to drive up the price is referred to as what? A. Bid siphoning B. Bid shielding C. Shill bidding D. Ghost bidding
g	What is a buffer-overflow attack? A. Overflowing a port with too many packets B. Putting more email in an email system than it can hold C. Overflowing the system D. Putting more data in a buffer than it can hold
h	Which of the following is not one of the basic types of firewalls? A. Screening firewall B. Application gateway C. Heuristic firewall D. Circuit-level gateway
i	What is a major weakness with a network host–based firewall? A. Its security is dependent on the underlying operating system. B. It is difficult to configure. C. It can be easily hacked. D. It is very expensive
j	What is the term for blocking an IP address that has been the source of suspicious activity? A. Preemptive blocking B. Intrusion deflection

	C. Proactive deflection D. Intrusion blocking
k	What method do most IDS software implementations use? A. Anomaly detection B. Preemptive blocking C. Intrusion deterrence D. Infiltration
l	SQL injection is based on what? A. Having database admin privileges B. Creating an SQL statement that is always true C. Creating an SQL statement that will force access D. Understanding web programming
m	Which of the following is a disadvantage to using an application gateway firewall? A. It is not very secure. B. It uses a great deal of resources. C. It can be difficult to configure. D. It can only work on router-based firewalls.
n	A person who hacks into phone systems is referred to as what? A. A hacker B. A gray hat hacker C. A phreaker D. A cracker
2.	**Solve the following questions**
a	Explain OSI Reference model in Detail?

b	Explain how can you Protect Against Investment Fraud and Identity Theft?
c	What is malware? Explain in detail
3.	**Solve the following questions**
a	What are trojan horses? Explain in detail
b	Explain the concept of VPN in detail?
c	How to protect yourself against cybercrime?
4	**Solve the following questions**
a.	Explain types and components of Firewall?
b	Elaborate the concept of Digital certificates in detail?
c	Explain the objectives of IT Act**?**
5	**Solve the following questions**
a	Explain the following 1) 4 categories of Auction Fraud 2) Bid Shielding 3) Bid Siphoning 4) Shill Bidding
b	Explain various virus scanning techniques?
c	Elaborate the concept of The Sassier Virus/Buffer Overflow in detail