DSVV

देव संस्कृति विश्वविद्यालय

शान्तिकुन्ज, हरिद्वार

उत्तर-पुस्तिका

परीक्षार्थी अनुक्रमांक (अंकों में) 1224014 पेपरकोड BCA-509
Student's Roll No. (in numbers) Paper code

परीक्षार्थी अनुक्रमांक (शब्दों में) Eighteen lakh twenty four thousand four teen नामांकन संख्या 1Q000.0013
Student's Roll No. (in words) Enrollment Number

कक्षा BCA-5th विषय Cyber Security
Class Subject

दिनाँक 08/12/2020 दिन Tuesday
Date Day

प्रश्न पत्र संख्या .....
Examination Paper Number

लघुत्तरीय A Short Answer Type							योग/Total
1	2	3	4	5	6	7	
दीर्घउत्तरीय B Long Answer Type							
1	2	3	4	5	6	7	
कुल योग अंकों में / TOTAL IN DIGITS							
कुल योग शब्दों में/TOTAL IN WORDS							

परीक्षक के हस्ताक्षर
Signature of Examiner

आवश्यक निर्देश / Important Instructions

1. उत्तर पुस्तिका में परीक्षार्थी अपना नामांकन क्रमांक केवल मुख्य पृष्ठ पर निर्धारित स्थान में ही लिखें अन्यत्र कहीं नहीं। Students must write their Enrollment Number on the Answer Booklet only at the prescribed place on the front page and nowhere else.
2. उत्तर पुस्तिका में परीक्षार्थी न तो कहीं अपना नाम लिखें और न ही कोई पहचान अंकित करें। Student should neither write their name in the Answer Booklet nor should they make any identification mark anywhere.
3. प्रश्न का क्रमांक सही और साफ-साफ लिखें। प्रश्न के खण्ड के साथ प्रश्न क्रमांक भी लिखें। Write the Question Number correctly and clearly. Write both the Section of the Question number.
4- एक प्रश्न का उत्तर समाप्त होने पर दूसरे प्रश्न का उत्तर नये पृष्ठ से ही प्रारम्भ करें। Start writing the answer of every question from a fresh page.
5- जिस प्रश्न को भी हल करें उत्तर पुस्तिका में उसे वही क्रम संख्या दें जो क्रम प्रश्न पत्र में दिया गया है। While answering the questions make sure that the Question number written in the Answer Booklet is the same as that given in the Question Paper.

Short Answer :-

Ans :- 1:- Difference between Cyber Crime and Cyber Terrorism :-

Cyber Crime :- The term cybercrime refers to online or Internet-based illegal acts. Today, cybercrime is one of the FBI's top three priorities.

Today, people rely on computers to create, store, and manage critical information.

Any illegal act involving a computer generally is referred to as a computer crime.

Cyber Terrorism :- A cyber terrorist is someone who uses the Internet or network to destroy or damage computers for political reasons.

The cyber terrorist might target the nation's air traffic control system, electricity-generating companies, or a telecommunications infrastructure.

	Cybercrime	Cyberterrorism
1.	Criminal activity done using a computer and network	1. Uses internet to carry out terrorist activities that deliberately causes large scale disruption of computer networks.
2.	Only towards certain individuals or selected victims	2. Towards a large scale of computers or institution due to political reasons
3.	Harmful towards people	Causes major disruption in computer networks which amounts to huge financial damages.
4.	Ex:- -spam -fraud (bank, identity theft -Obscene or offensive content -harassment -threats	4. Ex:- - mainly consists of sabotaging activites. - mass cyber attack.

Ans:-3 National Cyber Security Policy 2013:-

National Cyber Security Policy is a policy framework by Department of Electronics and Information Technology (DeitY, Now MietY). It aims at protecting the public and private infrastructure from cyber attacks.

The policy also intends to safeguard "information, such as personal information (of Web users), financial and banking information and sovereign data".

This was particularly relevant in the wake of US National Security Agency (NSA) leaks that suggested the US government agencies are spying on Indian users, who have no legal or technical safeguards against it.

India had no Cyber Security policy before 2013. This sparked a fusion among people. Under pressure, the government unveiled a National Cyber Security Policy 2013 on 2 July 2013.

Vision of this policy :- To build a secure and resilient cyberspace for citizens, business, and government and also to protect anyone from intervening in user's privacy.

Strategies of this policy :-

- Creating a secured Ecosystem
- Creating an assurance framework.
- Encouraging Open Standards.
- Strengthening The regulatory Framework.
- Securing E-Governance services.
- Promotion of Research and Development in cyber security.
- Reducing supply chain risks.
- Human ~~development~~ Resource Development.
- Creating cyber security awareness.
- Developing effective Public Private Partnership.
- Prioritized approach for implementation.

Ans:- 5:- International Convention on Cyberspace :-

The ~~third~~ Global Conference on Cyberspace are conferences held biennially since 2011 where governments, private sector and civil society gather to discuss and promote practical cooperation in cyber sapace, to enhance cyber capacity building and to discuss norms for responsible behavior in cyber space.

I will discuss the 5th Global conference on Cyber Sapace in 2017 organised by india in New delhi.

Prime Minister of India Mr. Narendra Modi will inaugurate the fifth edition of the Global Conference on CyberSpace, an official statement said. GCCS is one of the worlds largest conference on cyberspace.

The theme of the twoday conference is Cyber4All: A Secure and Inclusive Cyberspace for Sustainable Development.

Among the multiple transformative programs under digital India the biggest thing that India brings about to the table is Digital Inclusion that makes it sustainable and development which has been given utmost importance under the theme Cyber4All.

Goal and Benefits of GCCS-2017:-

- Goal of GCCS 2017 is to promote an inclusive Cyber Space with focus on policies and frameworks for security, safety & freedom.
- It will be an opportunity to showcase the "Digital India" program as a positive, sustainable and scalable model.
- It can help provide vision of inclusive digital socity for growth, education, helathcare especially for developing world.
- The plenary sessions and other activities during GCCS 2017 will be designed around the themes of Cyber4Inclusive Growth, Cyber4 Digital Inclusion, Cyber4 Security and Cyber4 Diplomacy.
- GCCS 2017 will bring forth the business empowerment and developmental potential of Cyber Space.
- Indian Start-ups will also get exposure to the global industry leaders and investors in GCCS 2017 to pitch their ideas through multiple seminars and exhibitions.

Ans:- 6:- Cyber Forensics with the real world case study:-

i) A person hosting obscene Profiles :-

State	Tamil Nadu
City	Chennai
Sections of law	67 of Information Technology. Act 2000 469, 509 of the Indian Penal code.

ii) "Nothing has really happened until it has been recorded" - Virginia Woolf

Background:- The complainant stated that some unknown person had created an e-mail ID using her name and had used this ID to post messages on five Web pages describing her as a call-girl along with her contact numbers.

As a result she started receiving a lot of offending calls from men.

Investigation :-

After the complainant heard about the Web pages with her contact details, she created a username to access and view these pages.

Using the same log in details, the investigating team accessed the Web pages where these profiles were uploaded. The message had been posted on five groups, one of which was a public group.

The investigating team obtained the access logs of the public group and the message to identify the IP addresses used to ~~the~~ post the message. Two IP address were identified.

The ISP was identified with the help of publicly available Internet site. They provided the names and address of two cyber cafes located in the Mumbai to the police.

The team also cross-examined the complainant in great detail During one of the meeting she revealed that she had refused a former collage mate who had proposed marriage.

In view of the above the former collage mate became the prime suspect. Using this information the investigating team, with the help of Mumbai police, arrested the suspect and seized a mobile

phone from him. After the forensic examination of the SIM card and the phone, it was observed that phone had the complainant's telephone numbers that was posted on the Internet. The owner of the cyber cafes also identified the suspect as the one who had visited the cyber cafes.

Based on the facts available with the police and the ~~xxx~~ sustain introgation the suspact confessed to the crime.

Current status:

The suspect was convicted of the crime and sentenced to two years of imprisonment as well as a fine.

Long Answer:-

Ans:- 1:- Security Steps for HTTP Applications and services:-

Web (HTTP) Application security is a the process of protecting websites and online services against different security threats that exploit vulnerabilities in an application's code.

Common targets for web application attacks are content management System, database administration tools and SaaS Applications.

→ Attack against web application range from targeted database to large scale network disruption are

- cross-site Scripting
- SQL Injection.
- Buffer overflow
- Data breach
- Cross-site request forgery (CSRF).
- Denial-of-Service (DOS)

Security steps for web (HTTP) Application and service:-

Web application security can be improved by protecting against DDoS, Application layer and DNS attack.

→ WAF (Web Application Firewall) Protect against application layer attac
A web application firewall or WAF does analyse both HTTPs and HTTPs web traffic, hence it can identify malicious hackers attacks because it works at the application layer.

→ Organization failing to secure their web applications run the risk of being attacked. Among other consequence, this can result in information theft, damaged client relation ships revoked licences and legal proccedings.

→ DDOS - protection. Our multi-tacted DDos mitigation services offer blanked protection against all network layer and application DDos attacks.

Imperva users can choose between DNS and BGP-enabled options to secure websites, web application and servers infrastructure.

- Bot filtering - Malicious bot are used in mass-scale automated assaults, accounting for over 90% of all application layer attacks.

→ Apart from a web application security scanner, you should also see use a network security scanner and other relevant tools to scan the web server and ensure that all services running on the server are secure. Security tools should be included in every administrator's toolbox

Ans:-4 Cyber security initiatives by the Government of India:-

~~Scenario~~ The cyber crime scenario in India:-

Some common cyber-crime scenarios which can attract prosecution as per the penalties and offences prescribed in IT Act 2000 (amended in 2008) Act

1:- Harassment via fake public profile on social networking site:- A fake profile of a person is created on a social networking site with the correct address, residential information or contact details.

2. Online hate community:- Online hate community is created inviting a religious group to act or pass objectionable remarks against

3. Email account hacking:- If victim's email account is hacked and obscene emails are sent to people in victim's address book.

4:- Credit Card fraud:- Unsuspecting victims would use infected computers to make online transactions.

5:- Cyber terrorism:- Many terrorists are using virtual and physic storage media for hiding information and records of their illicit business.

Cyber Security Initiatives by the Government of India.

The number of cyber security incidents has gradually increase in India over the last few years.

The government has taken certain cyber security initiatives as discussed below. more expansive and aggressive measures are required to meet the rising challenges.

Government Initiatives :-

National Cyber Security Policy, 2013 :- The Government of India took the first formalized step towards cyber security in 2013, vide the Ministry of Communication and Information Technology, Department of electronic and Information Technology's National Cyber Security Policy 2013.

The Policy is aimed at building a secure and resilent cyberspace for citizens, businesses and the Government. Its mission is to protect cyberspace information and infrastructure, build capabilities to prevent and respond to cyber attacks, and minimise damages through coordinated efforts of institutional structures, people, processes, and technology.

The objectives of the policy include creating a secure cyber ecosystem, compliance with global security standards, strengthen the regulatory framework, creating round the clock mechanisms for gathering intelligence and effective response,

Some of the strategies adopted by the Policy include:

- Creating a secure cyber ecosystem through measures such as a national nodal agency.
- Creating an assurance framework.
- Encouraging open standards.

→ In 2014, the PMO created the position of the National Cyber Security Coordinator.

→ Cyber Swachhta Kendra (Botnet cleaning and Malware Analysis center:- To combat cyber security violations and prevent their increase, Government of India's Computer Emergency Response Team (CERT-In) in February 2017 launched 'Cyber Swachhta Kendra' a new desktop and mobile security solution for cyber security in India.

ii Collaboration with industry Partners:- Development of Public Private Partnerships is an important strategy under the National CS Policy 201

→ International Cooperation Initiatives:-