NAME: HARSHADA A. RAJALE. MSE-1 SOLUTION

Sem 7 :- CSL (ILE)

VIT Vidyalankar Institute of Technology
(Accredited A+ by NAAC)
(Autonomous Institute Affiliated to University of Mumbai)

Mid Semester Examination

Branch	Date	Sem.	Roll No. / Exam Seat No.	Subject	Student's Signature	Junior Supervisor's Name and Sign
ALL	02/09/24	7	0674	CSL (ILE)		

Question No.	A	B	C	D	E	F	G	H	Total	Total out of (20 /30 / 40)
1										
2										
3										
4										

Examiners Signature	Student's Sign (After receiving the assessed answer sheet)

Q1

(A) Compare between Active attacks & passive attacks.

(I) Passive attack

① It involves monitoring or eavesdropping on the communication channel to gather information without altering the data or disrupting the system.

② It is harder to detect because the attacker does not interact with the system in a noticeable way.

③ While these attacks are potentially less immediately damaging, passive attacks can lead to significant steady security breaches if sensitive information is gathered & exploited later.

④ Encryption & secure communication

Scanned with CamScanner

protocols can help prevent unauthorised access to the data being transmitted

(5) Example of Passive attack:-
   (a) Eavesdropping
   (b) Traffic Analysis

(6) Tools used in Passive attacks:-
   (1) CheckUserNames
   (2) Google Earth
   (3) WHOIS
   (4) Nslookup
   (5) Dnsstuff

(B) Active Attacks:-
(1) It involves altering the data, disrupting communications, or gaining unauthorized access to a system. The attacker actively manipulates the network or data.
(2) It often causes immediate & visible damage, such as corrupted data, unauthorized actions, or system downtime.
(3) Generally considered more severe because it can cause direct harm to data & services
(4) Easier to detect because it involves noticeable changes in the network or system behavior.
(5) Examples of Active Attacks:-
   (a) Masquerade
   (b) Denial of Service (DoS)
(6) Tools used in active attacks:-
   (1) Arphound
   (2) Arping
   (3) Bing
   (4) Dig
   (5) Filesnarf.

Scanned with CamScanner

Q.1 b Role of Indian ITA 2000.

Role of Indian ITA 2000 in cyber security

① In India, Information Technology Act ITA 2000 was enacted after the United Nation General Assembly Resolution A/RES/51/162 is Jan 30, 1997.

② Cybercrimes are punishable under two categories :- ITA 2000 & IPC

- Section 43 :- Penalty for damage to computer.
  Fine :- Rs. 1 Crore
- Section 66 :- Hacking with computer system
  Fine :- Rs. 200000/- Imprisonment :- 3 years
- Section 68 :- Power of controller to directions
  Fine :- Rs. 100000/-, Imprisonment :- 5 years
- Section 72 :- Breach of confidentiality & privacy
  Fine :- Rs. 100000/-, Imprisonment :- Upto 2 years
- Section 73 :- False signature certificate.
  Fine :- Rs. 100000/-, Imprisonment :- 2 years.

Scanned with CamScanner

Q.1

(C) Security Gap & Team

(A) Security Gap

(1) The Security Gap Name :-
The situation describes Zero-Day Vulnerability

(2) It refers to a security flaw in software that is unknown to the software vendor or has no available fix or patch.

(B) Team Responsible :-

(1) The team responsible for resolving these vulnerabilities typically falls under the Incident Response Team or the Security Operations Center (SOC).

(2) Additionally, Vulnerability Management teams & Applications Security teams may work together to address the issue by developing temporary mitigations, workarounds, or collaborating with developers to create a patch.

Scanned with CamScanner

Q2 @ Cyber Criminals Plan the Attacks :-

Cyber criminals often plan their attacks through a series of well-structured steps designed to exploit vulnerabilities in systems, networks, or human behavior.

① Reconnaissance

① A reconnaissance attack occurs when an adversary tries to learn information about your network

② Reconnaissance is also known as Information Gathering

③ It is a preparatory phase to understand the system, its networking ports & services & other aspects of security, that are needful for launching the attacks.

ⓐ Passive attack

① It involves gathering information about the target without his/her knowledge.

② Criminals gather information without directly interacting with the target

③ It includes use of social media, public websites & online forums.

ⓑ Active attack

① It involves probing the network to discover individual hosts to confirm the information gathered in the passive attack phase.

② It can provide attackers about the confirmation of the security measures in place

③ The attackers develop or acquire tool &

Scanned with CamScanner

direct interaction with the target like scanning n/w for open ports, services & vulnerabilities.

Tools used in Passive attacks:
① CheckUserNames
② Google Earth
③ WHOIS
④ Nslookup
⑤ Traceroute.

Tools used in Active attacks.
① Arphound
② Hmap
③ Hunt
④ Nmap
⑤ TCPdump.

(II) Scanning & Scrutinizing gathered information
The key step to examine intelligently while gathering information about the target is scanning & scrutinizing gathered information.
The objectives are:
① Port Scanning
② Network Scanning
③ Vulnerability Scanning

① Port Scanning
- It is act of systematically scanning computer port
- The result of a scan on a port is usually generalised into one of the following categories:-
① Open or accepted

Scanned with CamScanner

② Closed or not listening
③ Filtered or Blocked

- Types of Port scan.
① Vanilla
② Strobe
③ UDP
④ Sweep
⑤ FTP bounce.

Port scanning is followed by vulnerability & network scanning.

② Scrutinizing
- Scrutinizing is always called the "Enumeration" in the hacking world
= The objective behind this is to identify:
- The valid user accounts / groups
- Network resources
- OS & different applications that are running on the OS.

• Usually most of the attackers consume 90% of the time in scanning, scrutinizing & gathering information on a target & only 10% of the time in launching the attack.

③ Launching an attack:
① After scanning & scrutinizing, the attack is launched using the following steps:
① Crack the password
② Exploit the privileges
③ Execute the malicious commands / applications

Scanned with CamScanner

④ Idide the files
⑤ Cover the tracks - delete the access logs, so that there is no trail illicit activity.

Q 2

(B) Classify cyber crime based on targets. Give example of each & explain one in detail.

The cybercrimes can be categorised in five different types based on the target:

① Cybercrime against Individual
② Cybercrime against property
③ Cybercrime against organization
④ Cybercrime against society
⑤ Crime emanating from Usent newsgroup.

(I) Cybercrime against Individual
① Email spoofing
② Phishing
③ Spamming
④ Cyberdefamation
⑤ Password sniffing

(II) Cybercrime against Property
① Credit card fraud
② Intellectual Property crime
③ Internet time theft

(III) Cybercrime against Organization
① Unauthorized accessing of computer
② Denial of Service attacks

Scanned with CamScanner

③ Logic bomb
④ Industrial spying
⑤ Software piracy

Ⓘ Cybercrime against society
① Forgery
② Cyber terrorism
③ Web Jacking
④ Ha

Ⓥ Crimes emanating from Usenet newsgroup
① Usenet newsgroup is a respository usually within the usenet system for message posted from many users in different location using Internet.
② Therefore, it is expected that one uses this with caution & common sense & exercise proper judgement as well as the skills at own risk

Explaination of Cybercrime:-
Ⓘ Unauthorized accessing of computer

① Unauthorized access is when someone gain access to a website program, server, service or other system using someone else's account or other method

Eg:- If someone kept guessing a password or username for an account that as not theirs until they gained access, it is considered as unauthorized access.

Scanned with CamScanner

To summarize, Unauthorised access to computer refers to act of gaining access to computer system, network or data without permission.

Scanned with CamScanner

Q3
(9) What is Bluetooth hacking. Explain different types of Bluetooth hacking.

(1) With the widespread adoption and convenience of Bluetooth device comes the inevitable implementation problems that cause unexpected things to happen.

(2) Some of the common attacks for hacking Bluetooth are Bluejacking, Bluesnarfing, Bluebugging & Car Whisperer.

1] Bluejacking
(1) This is very common & harmless kind of Bluetooth attack.
(2) This happens when a attacker searches for discoverable devices in the area & then sends spam in the form of text messages to devices.
(3) The best way to deal with the Bluejacking is to ignore the messages if you receive them.
(4) If you keep your Bluetooth settings to invisible or non-discoverable, you are not likely to receive these messages.

2] Bluesnarfing
(1) This is more serious than Bluejacking & can leave some of the private information stored on your smartphone open.
(2) The data can be accessed by

Scanned with CamScanner

hacking your device through Bluejacking.
③ The information stolen here may seem important to you but it might not be as precious as banking information

④ Bluebugging.
① If the hacker bluebugs your phone, he/she gains total access of control of your device.
② It makes hacker capable of accessing all information including photos, apps, contacts, etc.
③ This is feasible on older phones with outdated firmware.

⑤ Car Whisperer.
① Car whisperer is a hacking technique which can be used by attacker to hack hands-free Bluetooth in a car system. & connect to system to inject audio or record audio from a bypassing car.
② This attack takes advantage of the fact that most of the Bluetooth systems in cars need simple four digit security key & this key is not enough.
③ The use of default security key results in vulnerability

Scanned with CamScanner

Q3

(b) Considering the above scenario.

① Determine legitimacy.

(1) Verify the sender's email address for authenticity

(2) Manually type the bank's website URL to check your account.

② Red Flags:

(1) Look for urgent or threatening language

(2) Be cautious of unfamiliar or suspicious links & requests for sensitive information.

③ Suspected Phishing attempt.

(1) Avoid clicking on any links or opening any attachments.

(2) Report the email to your bank & delete it.

④ Protecting Yourself.

(1) Enable two-factor authentication (2FA)

(2) Keep your software & antivirus up to date.

⑤ After clicking a Phishing link.

(1) Immediately change passwords for affected accounts.

(2) Contact your bank to alert them & monitor your accounts.

Scanned with CamScanner