Name: Sachin Rajbhar
Rollno: 41221139
Class: BCA IV Sem

CSCL
Assignment 2
SOLUTIONS

18/05/23

Q1 Differentiate between DoS Attacks & DDoS attacks? (5)

	DoS Attack	DDoS Attacks
Source	Single device or computer	Multiple devices or computers (botnet)
Bandwidth	Limited by attacker's connection/device	Higher bandwidth due to multiple sources (amplification)
Vulnerability	Exploits vulnerability in the target system/network	Exploits vulnerabilities in third-party systems for amplification.
Detection	Relatively easier to detect	More challenging to detect due to the distributed nature.
Mitigation	Easier to mitigate	More challenging to mitigate due to distributed nature.
Attack Types	TCP/IP, application-layer attacks, resource exhaustion attacks	Various attack types with different characteristics
Attack Impact	More localized impact on a single target	Can impact multiple systems, services, or even entire networks
Attack Complexity	Simple execution with fewer resources & coordination	More complex due to involvement of botnets & coordination

SP

Q2 How do we prevent our applications from SQL injection attacks? (4)

Ans SQL injection is a type of cyber attack where an attacker inserts malicious SQL code into a query, exploiting the vulnerabilities in an application's input handling, to manipulate or extract data from a database.

- Some best practices to help protect your applications against SQL injection attacks.

1. Parameterized Queries / Prepared Statements: Instead of directly inserting user input into SQL queries, use special placeholders that are filled with sanitized user input (remove special coding characters)
2. Validate & sanitize user input: Check user input for length, format & allowed characters to prevent SQL injection.
3. Limit database privileges: Avoid using admin accounts for regular operations
4. Avoid exposing sensitive information: Do not reveal detailed error messages to users.
5. Encode input & output: Encoding techniques into user inputs & output
6. Keep Software up to date: Regular update database software & application frameworks
7. Implement a web application firewall (WAF): Use WAF to help detect & block malicious traffic.
8. Conduct security testing: Vulnerability scanning & penetration testing
9. Educate developers: Provide training & resources to development team for secure coding practices

Q3 Explain a case study on recent cyber attack in India? (5)

Ans Here is an example of recent cyberattack in India:

→ Date: January 2023
→ Target: Safdarjung Hospital in Delhi
→ Attack: Attackers used a phishing email to gain access to Safdarjung Hospital's network & steal patient data.
→ Impact: The attack compromised the personal data of over 10,000 patients, including their names, addresses & medical records.
→ Response: Safdarjung hospital has since taken steps to secure its network & is working to notify affected patients.

Here are some facts additional facts about the attack:
- The hackers were likely motivated by financial gain
- The attack was sophisticated & well-planned
- The Safdurjung Hospital is a major public hospital, & the attack highlights the vulnerability of India's public healthcare system to cyberattacks.

Here are some lessons learned from the attack
- Organisation need to be vigilant against phishing attacks.
- Organisations need to have robust cybersecurity measures.
- Organisation need a plan in place to respond such attacks.

Q4 Explain phishing & Spoofing. Which are the major types of spoofing? (5)

Ans ⇒ Phishing is a type of cyberattack in which attacker sends an email or text message that appears to be from a legitimate source, such as bank or gov. agency.
The email contains a link or attachment, if clicked on, install's malware on victim's computer.
This malware can be used to steal personal information such as passwords, CC numbers & Social security numbers.

⇒ Spoofing is a type of cyberattack in which the attacker alters the source of a communication to make it appear to come from a different source.
It can be used to make it from a legitimate company, when it's actually a fake website created by attacker.

The major types of spoofing are:-

- Email spoofing – Attacker alter's sender's mail address
- Caller ID spoofing – Attacker alter's caller ID info.
- IP spoofing – It alters the IP address to make it appear located in a different location.
- Website spoofing – Attacker creates a fake website that looks legit.

05 Write any two examples on eavesdropping attack

Two examples of eavesdropping attacks are:-

① Man-in-the-middle attack : In this, the attacker intercepts the communication between two parties & impersonates one of the parties. (intercept)

this allow the attacker to read all of the data that is being transmitted b/w the two parties.
He/She can modify & even manipulate data/message

② Wiretapping : It is a physical attack in which the attacker taps into the comm. line or wire to intercept the data that is transmitted.

this allow the attacker to read all the data also.
He/She cannot modify its content.

06 what is cross site scripting (XSS)

- Cross site scripting is a web application vulnerability that allows attackers to inject malicious scripts (usually in form of client-side code) into trusted websites used by other others.
- It occurs due to improper validation as user input sanitation allowing any arbitrary code to run in victim's browser.
- There are mainly three types :-
  - ① Stored XSS : Script is permanent saved on target server
  - ② Reflected XSS : Embedded in a URL or input field, when user clicks it get executed in their browser
  - ③ DOM-based XSS : Client side Javascript modifies the Document Object Model (DOM) of a web page, allows injecting malicious code affecting page structure.

4

07 What do you mean by blind SQL Injection?

- Blind SQL Injection is a type of SQL Injection Attack where the attacker can exploit a web application's database layer without direct feedback or error messages. They inject malicious code SQL into user input & analyze the application response indirectly to access data.

- 2 Major technique are :-
  ① Time-Based blind SQL Injection : Inject SQL queries to delay the response
  ② Boolean-Based-blind SQL Injection : Attacks constructs SQL queries resulting in true or false

- Preventive measures are :-
  1. Input Validation
  2. Parameterized queries
  3. Limited Database Access Privileges.

Name: Sachin Rajbhar
Class :- BCA IV Sem
Rollno: 4/22/139

CSCL
ASSIGNMENT 3
SOLUTIONS

11/08/23

Q1 Differentiate between hacking & cracking?

Hacking	Cracking
i) Hacking refers to the act of gaining unauthorized access to computer systems, networks, or devices with the intent of identifying vulnerabilities & improve security systems.	Cracking refers to the act of breaking or bypassing security measures, such as software licensing or copy protection with the intention of gaining unauthorized access.
ii) Hacking is often done with a positive intent to identify weakness & improve security systems.	Cracking is typically done with malicious intent to exploit vulnerabilities or gain unauthorized access.

Q2 How does a firewall protect data?

A firewall acts as a barrier b/w a trusted internal network & an untrusted external network. It helps protects data by implementing various security measures. Here's how a firewall protects data:

i) Packet Filtering : Firewall examine individual packets of data that flow through them & compare them against a set of predefined rules. By this, firewall prevents malicious traffic from reaching internal network.

ii) Access Control : Firewall enforce access control policies by allowing or denying specific types of network traffic. This helps protect data by limiting access to network resources.

iii) Network Address Translation (NAT) : Firewalls often use NAT to translate private IP address that are visible on the external network.

iv) Stateful Inspection : These firewalls maintain information about the state of network connections.

Q3 Briefly explain the IT infrastructure in India.

The IT infrastructure in India has experienced significant growth & development over the years.

i) Telecommunication Infrastructure :- India has a wide telecommunication network that includes wired & wireless connectivity options. It provides backbone of internet connectivity.

ii) Internet Connectivity :- India has witnessed a significant increase in internet penetration and access in recent years. Broadband internet service, both wired & wireless, are widely available in urban area.

iii) Data Centers : India has seen establishment of numerous data centers to meet the growing demand for storage, processing & hosting of digital data.

iv) E-Governance Infrastructure : The Indian government has undertaken various initiatives to digitise government services & improve governance through use of IT.

v) IT Education & Skilled workforce : India has a large pool of IT education system, that skilled workforce contributes to the development of India.

04 Explain any two national agencies handling IT in India.

Ans 1. National Informatics Centre (NIC)

↳ NIC is a premier science & technology organization under ministry of Electronics & Information Tech. (MeitY) in India.

↳ NIC develops & maintains IT infrastructure necessary for the operation of e-Governance projects & initiatives.

↳ NIC assists the design, development & implementation of e-Governance services & applications

↳ NIC conducts training programs & workshops to build the capacity of government officials & employees in & utilizing ICT Tools.

2. ↳ Computer Emergency Responsible Team - India (CERT-In):

↳ It is the national agency responsible for cybersecurity & handling cybersecurity incidents in India.

↳ It operates under the Ministry of Electronics & Information Technology (MeitY)

↳ It serves as the nodal agency for coordinating responses to cybersecurity incidents, analyzing threats & issuing alerts to govt organisations.

↳ It plays a crucial role in the prevention, detection & mitigation of cyber threats.

Q5 Write a short note on Birthday Attack.

A birthday attack is a cryptographic attack that exploits the birthday paradox to find collisions in a hash function. The birthday paradox states that in a group of just 23 people, there is 50% probability that two people will have same birthday.

The birthday attack lies in the fact that it reduces the security strength of a hash function. To mitigate it, cryptographic hash functions typically use larger hash output sizes & employ additional techniques such as salted hashes.

Q6 What is email security?

Email security refers to the measures & protocols in place to protect the confidentiality, integrity & availability of email messages & the associated data. Email is a widely used communication method for both personal & business purposes, ensuring its security is crucial to protect sensitive information.

Key aspects of email security are:-

i) Confidentiality
ii) Authentication
iii) Spam filtering & many more

Q7 What do you mean by security in operating system?

Security in Operating system refer to the measures, mechanisms & practices implemented to protect the confidentiality, integrity, & availability of the system & its resources. Operating system security aim to prevent unauthorized access, protect against malicious activities, & ensure the overall safety & reliability of the system.

Key aspects of security in Operating Systems:-

i) Access Control
ii) User Management
iii) File System Security
iv) Malware System Protection
v) Network Security
vi) Logging & Auditing