GROUP 1 - WEB-BASED PASSWORD CRACKING TECHNIQUES

Q&A

1. It is the process of determining the user's identity.

   a. Authentication
   b. Authorization
   c. Identification
   d. Calculation

2. What is the standard complexity for strong password?
   a. 12-digit password
   b. 14-digit password
   c. 8-digit password
   d. 16-digit password

3. What is hashing?

   a. It is the process of transforming any given key or a string of characters into another value.
   b. It is the act of compromising digital devices and networks through unauthorized access to an account or computer system.
   c. It is the extra bit of data in the URL after the question mark (?) that is used to pass variable.
   d. It is used to transfer data between client and server.

4. What a non-technical method could a cybercriminal use to gather sensitive information from an organization?

   a. Man-in-the-middle attack
   b. Social engineering
   c. Malware
   d. Pharming

5. All of the following are an example of hacking tools EXCEPT one.

   a. John the ripper
   b. Cain and Abel
   c. Botnet
   d. Nmap

GROUP 2 QUESTIONS

1. It is a technology that enables two or more entities to communicate without network cabling?

A. Local Area Network
B. Wireless Network
C. Virtual Private Network
D. Virtual Local Network

2. Is a group of device manufacturers that developed a standard for transmitting data via infrared (IR) light waves?

A. IrDA (Infrared Data Association)
B. Bluetooth
C. HomeRF
D. WIRELESS FIDELITY (WI-FI)

3. HomeRF is an alliance of businesses that have developed a standard called _____.

A. Digital Enhanced Cordless Telecommunications (DECT)
B. Shared Wireless Access Protocol (SWAP)
C. WIRELESS FIDELITY (WI-FI)
D. Bluetooth

4. Is a network card which connects to a wireless radio-based network?

A. WIRELESS NICs
B. Router
C. Modem
D. Access points

5. A device that receives and sends data on computer networks?

A. Modem
B. Access points
C. WIRELESS NICs
D. Router

GROUP 3 (QUESTION AND ANSWER)

1. The practice and study of hiding information.

   a. Criptography
   b. Crypgography
   c. Cryptography
   d. Crepetograpy
   e. Cripetograpy

2. The process of proving one's identity.

   a. Privacy
   b. Confidentiality
   c. Integrity
   d. Authentication
   e. Receiver

3. Ensuring that no one can read the message except the intended receiver.

   a. Privacy
   b. Confidentiality
   c. Address
   d. Host
   e. Message

4. A mechanism to prove that the sender really sent this message.

   a. Non-Repudiation
   b. Sender
   c. Integrity
   d. Secret Key
   e. Public Key

5. The receiver that the received message has not been altered in any way from the original.

   a. Public Key
   b. Private Key
   c. Asymmetric
   d. Symmetric
   e. Integrity

BSIT 4-2 Group 4 – Virus and Worms

Questions with Answers

1. It is a type of malware that is attached to another file. The malicious code automatically makes copies of itself and drops its payload when the host file is opened.

   A. Worm
   B. Virus
   C. Ransomware
   D. Trojan

2. It spreads across a network through your Internet or LAN (Local Area Network) connection.

   A. Worm
   B. Virus
   C. Ransomware
   D. Trojan

3. Which of these are not part of the Virus Detection Methods?

   A. Scanning
   B. Interception
   C. Heuristic Checking
   D. Filtering

4. This type of virus works by using the empty sections of a file to house a virus, without altering its actual size.

   A. Polymorphic Virus
   B. Multipartite Virus
   C. Space filler Virus
   D. Boot Virus

5. This type of worm encrypts data on the victim's system. It is commonly used in ransomware attacks, where perpetrators demand payment in exchange for a key to decrypt the files.

   A. Instant Messaging Worms
   B. Internet Worms
   C. Cryptoworms
   D. Email Worms

GROUP 5: WEB APPLICATION VULNERABILITIES

1. It refers to the flaws or weaknesses in an application that can lead to exploitation or a security breach.
    a. Vulnerabilities
    b. Web Application Vulnerabilities
    c. Operating System Vulnerabilities
    d. Security Vulnerabilities

2. What is biggest drivers behind the vulnerability of web applications?
    a. Security Setting Misconfigurations
    b. Failures in the design
    c. Configuration of an application
    d. Software and Data Integrity Failures

3. Which of the following is NOT a phase of Web Application Penetration Testing?
    a. Reconnaissance
    b. Discovery
    c. Implementation
    d. Exploitation

4. What is the common type of vulnerability in which attackers trick a web application into running or exposing files on a web server?
    a. Local File Inclusion (LFI)
    b. Directory Traversal
    c. Security Misconfigurations
    d. Cross-Site Scripting (XSS)

5. What do you call the application security testing methodology in which the application is tested in operating mode from the front-end to find vulnerabilities through simulated attacks?
    a. Interactive Application Security testing (IAST)
    b. Static Application Security Testing (SAST)
    c. Extended Detection and Response (XDR)
    d. Dynamic Application Security Testing (DAST)

Group 6 - SQL Injection

1. It is an attack that consists of insertion of a SQL query via the input data from the client to the application.
   A. Vaccine injection
   B. SQL injection
   C. Laboratory injection
   D. PHP injection

2. He is a security technology professional with over a decade of experience in the security industry with a pseudonym of “Rain Forest Puppy.” He also documented the first SQL injection exploit in 1998.
   A. Jeff Cornristal
   B. Jefferson Dongtai
   C. Jeff Forristal
   D. Thomas Jefferson

3. This technique takes advantage of the UNION SQL operator, which fuses multiple select statements generated by the database to get a single HTTP response.
   A. Union-based SQL injection
   B. Boolean
   C. Error-based SQL injection
   D. Out-of-band SQL injection

4. An attacker sends a SQL query to the database, which makes the database wait before it can react. The attacker can see from the time the database takes to respond, whether a query is true or false.
   A. In-band SQL injection
   B. Union-based SQL injection
   C. Out-of-band SQL injection
   D. Time-based

5. It allows a client to identify the database with which they are attempting to communicate with, when connecting to a database server or cluster with multiple database instances.
   A. Oracle Virtual Machine
   B. SQL Server Resolution Service
   C. Microsoft Azure & 365
   D. BBQSQL

Group 7: Questionnaire

1. Which of the following are not forms of firewalls?
   - **a.** Packet-Filtering Firewall
   - **b.** Circuit-Level Gateway
   - **c.** Stateful Inspection Gateway
   - **d. Secure Email Gateway**

2. In the Demonstration of Group 7, In what type of firewall does the proxy server include?
   - **a.** Circuit-Level Gateway
   - **b. Application-Level Gateway**
   - **c.** Stateful Inspection Gateway
   - **d.** Secure Email Gateway

3. In the types of IDS alerts, what is the “attack but no alert”?
   - **a.** True Positive
   - **b. False Negative**
   - **c.** False Positive
   - **d.** True Negative

4. What are the hackers typically use to bypass IDS?
   - **a. TTL Attacks**
   - **b.** Overlapping Fragments
   - **c.** DoS Attacks
   - **d.** Insertion Attacks

5. Deployed and used to gain a better understanding of attack techniques, motivations, information about malware strains in the wild, and security vulnerabilities.
   - **a.** High Interaction Honeypots
   - **b. Research Honeypots**
   - **c.** Low Interaction Honeypots
   - **d.** Medium Interaction Honeypots

GROUP 8 – LINUX HACKING

1. Who created Linux?
    a. Linux Torvalds
    b. **Linus Torvalds**
    c. Linus Thorvalds
    d. Linux Thorvald

2. An open-source network scanner that is used to recon/scan networks. It is used to discover hosts, ports, and services along with their versions over a network. It sends packets to the host and then analyzes the responses in order to produce the desired results.

    a. Rainbow Cracker
    b. Angry IP Scanner
    c. **Nmap**
    d. Arp-scan

3. A procedure for identifying active hosts on a network, either for the purpose of attacking them or for network security assessment.

    a. Network Scanning
    b. Linux Vulnerability scanning
    c. Password cracking
    d. Penetration testing

4. Software developed for decoding passwords in a variety of formats, such as encrypted or hashed passwords.

    a. Network Scanning
    b. Linux Vulnerability scanning
    c. Password cracking
    d. Penetration testing

5. It Monitors network traffic for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for harmful activity or policy breaching.
    a. Password Cracker
    b. Technical Linux Auditing Tools
    c. Wireless Sniffer
    d. **Intrusion Detection Systems**

Group 9: BUFFER OVERFLOW

1. This type of shellcode downloads and executes a specified file on the target system. This can be used to download and execute a malicious payload, such as malware.

   a. Message box shellcode
   b. Shellcode to spawn a new process
   c. Download and execute shellcode.
   d. Bind shellcode

2. A program or process attempts to store more data in a buffer (a temporary data storage area) than it was designed to hold called?

   a. Buffer Overflow
   b. NOPS
   c. Shellcode
   d. Countermeasure

3. What is a counter measures?

   a. Is a measure or action taken to prevent or counteract a particular threat or vulnerability?
   b. is a list of carefully crafted instructions that can be executed once the code is injected into a running application – like a virus inside a cell – but it isn't really a standalone executable program.
   c. is an assembly language instruction, programming language statement, or protocol command that does nothing.
   d. Is a small piece of code used as the payload in the exploitation of a software vulnerability.

4. NOPS is called?

   a. No Orientations
   b. No Operations
   c. No Options
   d. No Protocols

5. Small piece of code, often written in assembly language, that is used to exploit a software vulnerability in order to run arbitrary code on a target machine.

   a. Bind shellcode
   b. Counter Measure
   c. Remote Shellcode

d. Shellcode

Grp 10: Pen test methods

1. Which is NOT one of the common vulnerabilities that a pen test can uncover
    a. Insecure setup or configuration of networks, hosts and devices
    b. Flaws in encryption and authentication
    c. Code and command injection
    d. Possible attacks by hackers

2. Simulates how an experienced threat actor would perform a hack. It starts with no knowledge or understanding of the target's technology infrastructure and security provisions.
    a. White box
    b. Black box
    c. White box
    d. Opaque box

3. It can be further subdivided into two categories: external tests and internal tests.
    a. Wireless network pen test
    b. Client-slide pen test
    c. Web app pen test
    d. Network penetration pen test

4. Testers search security problems associated with the insecure design, development, or coding of a web app.
    a. Wireless network pen test
    b. Client-slide pen test
    c. Web app pen test
    d. Network penetration pen test

5. It can identify security vulnerabilities within an organization.
    a. Wireless network pen test
    b. Client-slide pen test
    c. Web app pen test
    d. Network penetration pen test