B.SC COMPUTER SCIENCE

FIRST SEMESTER EXAMINATIONS: 2016/2017

CSCD 431: DATA NETWORK SECURITY II

SECTION A:

INSRUCTIONS

ANSWER ANY THREE OF THE QUESTIONS FOR 15 MARKS EACH

TIME ALLOWED: ***TWO AND A HALF (2½) HOURS***

[60 MARKS TOTAL]

Time Allowed: 2:30 hours **Total Marks: 60**

INSTRUCTIONS:

1. In the Network Security Model, the TCP/IP has Four Abstraction Layers. Explain the threat, vulnerabilities and the probable attacks that can be initiated on each layer when it is not configured properly. [8 MARKS]

ANSWER

The link layer (commonly Ethernet) contains communication technologies for a local network. Vulnerabilities, Hub, Switches, brute force attack on network, Access control vulnerabilities

The internet layer (IP) connects local networks, thus establishing internetworking.
Vulnerabilities includes Attaches on IP Address, Firewall Synchronization Attack or Sync Flooding.

The transport layer (TCP) handles host-to-host communication. Layer establishes communication from web browser to the Web server. Without SSL and TLS others
Vulnerabilities includes Cross site scripting attacks, Cross site request forgery and side jacking or session high jacking.

The application layer (for example HTTP) contains all protocols for specific data communications services on a process-to-process level (for example how a web browser communicates with a web server). Web browser attaches in URL from client side and server side.

B, Define ethical hacking and the rationale behind it. [7 MARKS]

ANSWER 1B

An ethical hacker possesses the skills, mindset, and tools of a hacker but is also trustworthy.
Ethical hackers perform the hacks as security tests for their systems.

- If you perform ethical hacking tests for customers or simply wants to add another certification to your credentials.
- Ethical hacking also known as Penetration testing or white-hat hacking involves the same tools, tricks, and techniques that hackers use**, but with one major difference.**
- Ethical hacking is legal.
- Ethical hacking is performed with the target's permission.
- The intent of ethical hacking is to discover vulnerabilities from a hacker's viewpoint so systems can be better secured.
- It's part of an overall information risk management program that allows for ongoing security improvements.
- Ethical hacking can also ensure that vendors' claims about the security of their product

2. Explain the difference between WEP and WPA/2. With examples give reason why you would se lect one against the other. [10 Marks]

ANSWER

WEP (Wireless Equivalency Protocol)

WAP (Wireless Access Point)

WEP is not the best protection AND Generally not as secure as the more sophisticated WPA/WPA2 encryption.

- If a hacker can sniff packets on a WEP encrypted network, it is only a matter of time until the password is cracked.
- If enough traffic can be intercepted by an attacker, then it can be broken by brute force. E.g. Two Nigerians and the CID
- The time it takes to crack WEP only grows linearly with key length
- A 104-bit key doesn't provide any significant protection over a 40-bit key when faced against a determined cracker.

Shared Key and Open System Authentications

In Shared Key, the client request authentication and the Wireless Access Point sends a text which the client has to encrypt using the WEP key and send it back

- If it matches then the WAP (Wireless Access Point) authenticates and associates it with the client.

In Open System Authentication any client can associate with WAP

- The client is authenticated regardless of the key it possesses and begins to receive packets.
- The client would need the correct key at this point to read the packets.
- A WEP key is usually 128bit comprised of 26 hexadecimal values and a 24bit Initialization Vector (IV).
- Each packet is encrypted using RC4 algorithm with the 26 hexadecimal values and a random IV.
- The packet is sent along with the IV in plain text.
- The client then decrypts the packet using the hex key and the included IV.

Wi-Fi Protected Access (WPA) is a software/firmware improvement over WEP.

- All regular WLAN-equipment that worked with WEP are able to be simply upgraded and no new equipment needs to be bought.
- WPA is a trimmed-down version of the 802.11i security standard that was developed by the IEEE 802.11 to replace WEP.
- TKIP (Temporal Key Integrity Protocol) encryption algorithm was developed for WPA to provide improvements to WEP that could be fielded as firmware upgrades to existing 802.11 devices.
- The WPA profile also provides optional support for the AES-CCMP algorithm that is the preferred algorithm in 802.11i and WPA2.

B, Explain the following kali Linux penetration testing software (Aircrack-ng) suite commands used in WEP and WPA Security. [5 Marks]

ANSWER 2B

kali Linux Penetration Testing Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless LANs.

- It works with any wireless network interface controller whose driver supports raw monitoring mode and can sniff:
    - 802.11b
    - 802.11g
    - 802.11n traffic
- The program runs under Linux and Windows.

ANSWER

The Kali Linux Pentest software commands suite includes:

- aircrack-ng - Cracks WEP and WPA (Dictionary attack) key
- airdecap-ng - Decrypts WEP or WPA encrypted capture files with known key.
- airmon-ng - Placing different cards in monitor mode.
- aireplay-ng - Packet injector (Linux, and Windows).
- airodump-ng - Packet sniffer: Places air traffic into PCAP or IVS files and shows information about networks.

3. Define Network Security Management and briefly explains its importance to the following and where probable use examples to justify the answer. [8 Marks]

- Business Continuity Planning
- Business Process Reengineering
- Information Assurance

ANSWER

Network Security Management is the process of designing a security policy that will help to enforce an organization's systems user (Most Difficult task) from gaining unauthorised access.

- To specify an organization's information protection requirements, access controls, and audit requirements.

- It involves the process of restoring the system back in the event of failure e.g. (power supply, hardware, software, etc)

Business Continuity Planning -"identifies an organization's exposure to internal and external threats and synthesizes hard and soft assets to provide effective prevention and recovery for the organization, while maintaining competitive advantage and value system integrity".

Business Process Reengineering - is the analysis and design of workflows and processes. A logically related tasks performed to achieve a defined business outcome.

Information Assurance - the practice of assuring information and managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes. Assurance focuses on the reasons for assurance that information is protected and ensures business continuity process.

b. With the aid of a diagram explain the three security objectives and threat issues? [7Marks]

ANSWER 3B

The CIA triad gives us a model that explains security concepts, and tends to be very focus on security as it pertains to data.

The confidentiality, integrity, and availability triad.

- Confidentiality
    - "Preserving authorized restriction on information access and disclosure, including means for protecting personal privacy and proprietary information." Confidentiality of ATM PIN Number, Account Information
- Integrity
    - "Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity." E.g ensure information is correct

- Availability
    - "Ensuring timely and reliable access and use of information."
    - E.g. have my information whenever I need them 24/7

4. Briefly explain the three main techniques hackers or crackers can use to cause damage on networks? [7 Marks]

ANSWER

Cracking techniques on networks include:

- Creating worms - Computer worms are malicious software applications designed to spread via computer networks.
    - Computer worms are one form of malware along with viruses and trojans.
- Initiating denial of service (DoS)attacks - refers to a form of attacking computer systems over a network. DoS is normally a malicious attempt to render a networked system unusable (though often without permanently damaging it).
- Establishing unauthorized remote access connections to a device. Such as: Interruption, Interception, Modification and Fabrication

b. With the aid of a diagram, briefly explain the four main security threats that a hacker can remotely cause on a network. [8 Marks]

ANSWER 4B

Interception means that some unauthorized party has gained access to an asset.

- The outside party can be a person, a program, or a computing system.
- Examples of this type of failure are illicit copying of program or data files, or wiretapping to obtain data in a network.
- Although a loss may be discovered fairly quickly, a silent interceptor may leave no traces by which the interception can be readily detected.

Interruption, an asset of the system becomes lost, unavailable, or unusable.

- An example is malicious destruction of a hardware device, erasure of a program or data file, or malfunction of an operating system file manager so that it cannot find a particular disk file.

Modification - is a type of treat an unauthorized party not only accesses but tampers with an asset.

- For example, someone might change the values in a database, alter a program so that it performs an additional computation, or modify data being transmitted electronically.
- It is even possible to modify hardware. Some cases of modification can be detected with simple measures, but other, more subtle, changes may be almost impossible to detect.

Fabrication is where an unauthorized party might create a copy of counterfeit objects on a computing system.

- The intruder may insert spurious transactions to a network communication system or add records to an existing database.

- Sometimes these additions can be detected as forgeries, but if skillfully done, they are virtually indistinguishable from the real thing.

4. With examples explain the five Information/Data Security Governance? [7 Marks]

b. As a Systems Administrator, list and briefly explain the security "Best Practices" that is required to ensure Data Security in Network Environment? [10Marks]

ANSWER

- Standards: Functional specific mandatory activities, actions, and rules. E,g. ISO27001/2. International Standard Organization. ISO9001. Quality Assurance. OWASP, NIST
- Policy: Management directives that establish expectations (goals & objectives), and assign roles & responsibilities. Derived from ISO
- Process: Step-by-step implementation instructions when configuring a security system. Determined by nature of business e,g, Bank will be different from Hospital
- Procedure: Laid down rules that employers are to follow. Rules of Authorization rights.
- Guideline: General statement, framework, or recommendations to augment process or procedure

ANSWER B

b. List the eight Data Security "best practices"? [5Marks]

The eight security "best practices"?

I. Confidentiality

II. Integrity

III. Availability

IV. Need to know

V. Least privilege

VI. Separation of duties

VII. Job rotation

VIII. Mandatory vacation