Section A Multiple Choice (1 mark each)

1. Scapy does *not* support the ___________ of packets.
   a. decoding
   b. interpreting
   c. visual inspection
   d. manipulation

2. What is the difference between the *show()* and *show2()* commands in Scapy?
   a. *show()* displays packet info. filtered with a λ-function
   b. *show2()* displays the graph of all conversations
   c. *show2()* gives a detailed view of the packet but on an assembled packet
   d. *show()* gives a detailed view of the packet but on assembled packet

3. The command *a = IP(ttl = [10, 11, (12,14)])* creates:
   a. 4 packets with ttl of 10, 11, 12 and 14
   b. 5 packets with ttl of 10, 11, 12, 13 and 14
   c. 2 packets with ttl of 10 and 11 and default values of 12 and 14 respectively
   d. 3 packets with ttl of 12, 13 and 14

4. In Click, the *Tee(n)* command:
   a. Deletes the first *n* bytes from a packet
   b. Stores at most *n* packets
   c. Sends packets to all *n* outputs
   d. Sets the paint annotation to *n*

5. Pull calls in Click:
   a. Return NULLIFY if there is no packet
   b. Can be re-scheduled with the use of timer
   c. Can be triggered by the packet-downstream event
   d. Always pass a packet object

6. Which standard is used for digital certificates?
   a. ANSI
   b. Kerberos
   c. X.509v3
   d. ASCII

7. Which of the following is used by certification authorities to digitally sign certificates?
   a. Public key of the certification authority
   b. Private key of the certification authority
   c. Private key of the receiver
   d. Both a and c

8. How are trust relationships created in Windows Server 2008?
   a. Manually only
   b. Automatically only
   c. Manually or automatically
   d. Semi-automatically

9. Forest trusts can be created between ___________ forests.
   a. **only two**
   b. a maximum of three
   c. an unlimited number of
   d. a maximum of ten

10. ADSI stands for ___________.
   a. Active Decryption Services Interfaces
   b. Active Directory System Interfaces
   c. Active Device Services Interfaces
   d. **Active Directory Services Interfaces**

11. How can user accounts be created in a Windows Server environment?
   a. **Manually using Active Directory**
   b. Using a VBScript script only
   c. Using an account compiler
   d. Either a or b

12. Which authentication mechanism is used by Windows NT SP4 clients?
   a. Kerberos
   b. **NTLM2**
   c. LM
   d. NTLM

13. Which of the following is *not* a part of the account lockout policies in Windows?
   a. Account lockout threshold
   b. **Account lockout password**
   c. Reset account lockout counter after
   d. Account lockout duration

14. Which security template is created when a computer running Windows Server 2008 is promoted to a domain controller?
   a. dcsecure.inf
   b. security.inf
   c. securedc.inf
   d. **None of the above**

15. The type of secure communication between a sender and receiver can be decided using:
   a. IPSec Blocking Policy
   b. IPSec Permit Policy
   c. **IPSec Negotiation Policy**
   d. IPSec Deny Policy

16. The Layer 2 Tunneling Protocol uses ___________ for data encryption.
   a. **IPSec**
   b. PPTP
   c. Microsoft Point-to-Point Encryption
   d. PPTP/IPSecs

17. Which of the following is a characteristic of Wi-Fi Protected Access (WPA)?
    a. Employs a 32 bit initialization vector
    b. Uses a static encryption key
    c. An improvement of WEP
    d. Employs a 12 bit initialization vector

18. Which technology is *not* designed to protect data in transit over a network?
    a. Secure Sockets Layer (or TLS)
    b. Encrypting File System (EFS)
    c. IPSec
    d. Virtual Private Networks (VPNs)

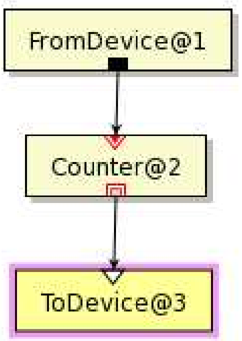
19. A Wireless Personal Area Network (WPAN):
    a. Has a range of approximately 500 meters
    b. Covers a greater range than WLAN
    c. Has a range of about 10 meters
    d. None of the above

20. Two or more wireless devices communicating directly with each other is an example of a(n):
    a. Infrastructure network
    b. Topology network
    c. Ad hoc network
    d. Mesh node structure

Section B Short Answer (15 marks)

Answer ONLY 5 from the following questions (3 marks each)

Explain what is wrong in the Click router example below and how it can be fixed.



Error: the counter element cannot act as both a push and pull at the same time. (1.5 marks)

Solution: using a queue for push-to-pull transition, i.e. between the FromDevice and Counter elements. (1.5 marks)

Explain the various Windows authentication mechanisms: LM, NTLM (v1 and v2) and Kerberos.

LM (LAN Manager) (1 mark)

- **Used by Windows NT and Windows 9x clients simultaneously with NTLM**
- **Low security**

NTLM (NT LAN Manager) (0.5 mark)

- **Used by Windows NT and Windows 9x clients**
- **Used by Windows 2000, 2003, and XP clients in certain situations, such as when logging on to a Windows NT domain**
- **Moderate security**

NTLM2 (NT LAN Manager version 2) (0.5 mark)

- **Used by Windows NT SP4 clients**
- **Used by Windows 9x clients with Directory Services Client installed**
- **Used by Windows 2000, 2003, and XP clients in certain situations**
- **High security**

Kerberos (1 mark)

- **Used by Windows 2000, 2003, and XP when logging on to a Windows 2000 or Windows Server 2003 domain**
- **Optimal security**

Describe three types of messages that are logged by the System Event Log.

Any 3 from the list below, 1 mark for each

Information

- **Successful operation of a task e.g. driver loaded**

Warning

- **May indicate a future problem e.g. low disk space**

Error

- **Indicate significant problem e.g. failure to load a service**

Failure (Security log)

- **Failure of an audited security event e.g. user cannot access NW drive**

Success (Security log)

- **Success of an audited security event e.g. user logs on computer**

Define what a security template is and give two of its advantages?

Security templates = a collection of security configuration settings. (1 mark)

Advantages (any 2 from list below for 2 marks):
1. STs are plain text files: easy to work with and modify the text file
2. STs make it easy to store security configurations of various types so that you can easily apply different levels of security to computers performing different roles
3. Save ST containing original settings → simply apply it to the GPO to return to default settings

List 6 countermeasures that can be taken to help secure a wireless network.

Any 6 from list below, 0.5 mark each:

- **Knowing the hacking methods to protect from holes**
- **Configure the AP correctly**
- **Change the default SSID**
- **Change default password**
- **Change SNMP community string**
- **Enforce authentication/authorization mechanism**
- **Firewall, packet filter in gateways, routers between AP and intranet**
- **Prevent physical access**
- **Protect building from interference**
- **Use MAC address filters**
- **Use Dynamic WEP keys with 802.1x**
- **Use Message Integrity Checksum (MIC) for data confidentiality and integrity**

Footprinting is a common attack against a DNS Server. Explain what happens in this type of attack?

- **DNS zone data obtained by an attacker to provide the attacker with the DNS domain names, computer names, and IP addresses for sensitive network resources = begins attack by using this DNS data to footprint network**
- **Usually DNS domain and computer names indicate the function or location of a domain or computer attacker takes advantage of DNS principle to learn the function or location of domains and computers in network**

(3 marks for complete answer)

Section C Long Answer (15 marks)
Answer ALL questions in this section (5 marks each)

1. Explain any five of the eight main trust types (i.e. tree-root, parent-child, short-cut, realm, external, forest, incoming and outgoing).

Any 5 from list below, 1 mark for each:

Tree-root trust:

- **Automatically established when a new tree root domain added to an existing forest.**
- **TR is transitive and two-way.**

Parent-child trust:

- **Automatically established when a new child domain added to an existing tree.**
- **TR transitive and two-way.**

Shortcut trust:

- **TR manually created by systems administrators (SAs).**
- **These trusts can be defined between any two domains in a forest.**
- **Generally for improving user logon & resource access performance.**
- **Useful when users in one domain needs to access resources in another domain.**
- **Shortcut TRs are transitive and can be configured as one-way or two-way.**

Realm trust:

- **Manually created by SAs between a non–Windows Kerberos realm and a WS2008 AD domain.**
- **Provides cross-platform interoperability with security services.**

- **Either transitive or non-transitive, and one-way or two-way.**

External trust:

- **Manually created by SAs between AD domains in different forests…**
- **Or between a WS2008 AD domain and a Windows NT 4.0 domain.**
- **Non-transitive and can be configured as either one-way or two-way.**

Forest trust:

- **Manually created by SAs between forest root domains in two separate forests.**
- **If a forest TR is two-way, it effectively allows authentication requests from users in one forest to reach another, and for users in either forest to access resources in both.**
- **Forest TR are transitive between two forests only and can be configured as either one-way or two-way as needed.**

Incoming Trust:

- **When a SA in the trusted domain is establishing the TR, trust is considered incoming trust.**
- **Before accessing resources in the trusting domain, users must be authenticated.**

Outgoing Trust:

- **When a SA in the trusting domain is establishing the TR, trust is considered outgoing.**
- **Before accessing resources in the domain, users from the trusted domain can be authenticated by passing authentication through to the trusted domain.**

2. Explain what is recorded by the Windows logs below.

   Application log **(1 mark)**

   - **Information/errors/warnings by the applications on a computer**
   - **For example, file error of a DB program might record a file error**
   - **Program owner decide which events to monitor**

   Security log **(1 mark)**

   - **Valid and invalid logon attempts, and resource usage: events related to creating, opening, or deleting files or other objects**
   - **Specify by administrator**
   - **For example, if logon auditing attempts enabled ð auditing entries**
   - **After auditing configuration, use log to track unauthorized access to objects**

   System log **(1 mark)**

   - **Information/errors/warnings by Win XP OS**
   - **Example: if trouble to start a service, look at these logs or if driver failures**

   Directory Service log **(1 mark)**

   - **Information/errors/warnings by AD**
   - **Only on domain controllers**

   DNS Server log **(1 mark)**

   - **Information/errors/ warnings by the DNS server**

3. (a) Denial of Service attacks can bring down a wireless network and disrupt the service. These attacks can happen from two different levels: the physical level and the protocol level. Describe the attacks at each of these two levels.

Physical level **(1.5 marks)**

- **Physical destruction of AP after locating AP**
- **Or physical destruction of antenna after locating antenna**
- **Signal of the 802.11b wireless network can be disrupted by the microwave in the kitchen (i.e. interference)**
- **Or the new 2.4 GHz digital cordless phones. (i.e. interference)**

Protocol level **(1.5 marks)**

- **An attacker can disrupt service from the protocol level.**
- **When establishing associations to use the wireless network, if you can build an association, then there must be a way to disassociate.**
- **If you can authenticate, then there must be a way to unauthenticate.**
- **802.11b standard, both methods exist, and both methods do not require any authentication in the message.**
- **Means the attacker can send out a disassociate or unauthenticate message to an arbitrary wireless network user and disconnect them. This is a bad design aspect of the protocol.**

(b) Besides a Denial of Service attack, list two other active attacks against a wireless network (you don't need to describe them).

- **Fake access point (1 mark)**
- **Theft of WEP key from user's laptop (1 mark)**