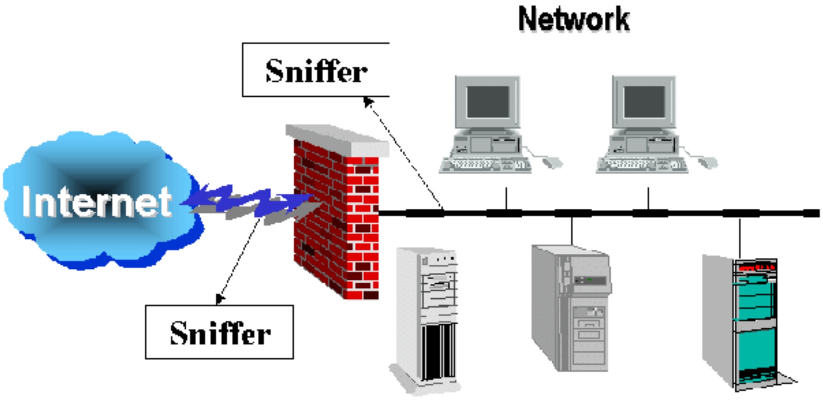
Each question carries 4 marks

Q.1. What is ARP spoofing and Packet sniffing? Explain

ARP spoofing

- ARP is used to resolve IP addresses to MAC addresses.
- In an ARP spoofing attack, a malicious party sends spoofed ARP messages across a local area network in order to link the attacker's MAC address with the IP address of a legitimate member of the network.
- This type of spoofing attack results in data that is intended for the host's IP address getting sent to the attacker instead.
- Malicious parties commonly use ARP spoofing to:-
  - steal information
  - modify data-in-transit or
  - stop traffic on a LAN.
- ARP spoofing attacks can also be used to facilitate other types of attacks, including:
  - denial-of-service,
  - session hijacking and
  - man-in-the-middle attacks.

Packet sniffing



- Packet sniffing is a technique of capturing packets that flows in the network
- The software or device used to do this is called a packet sniffer.

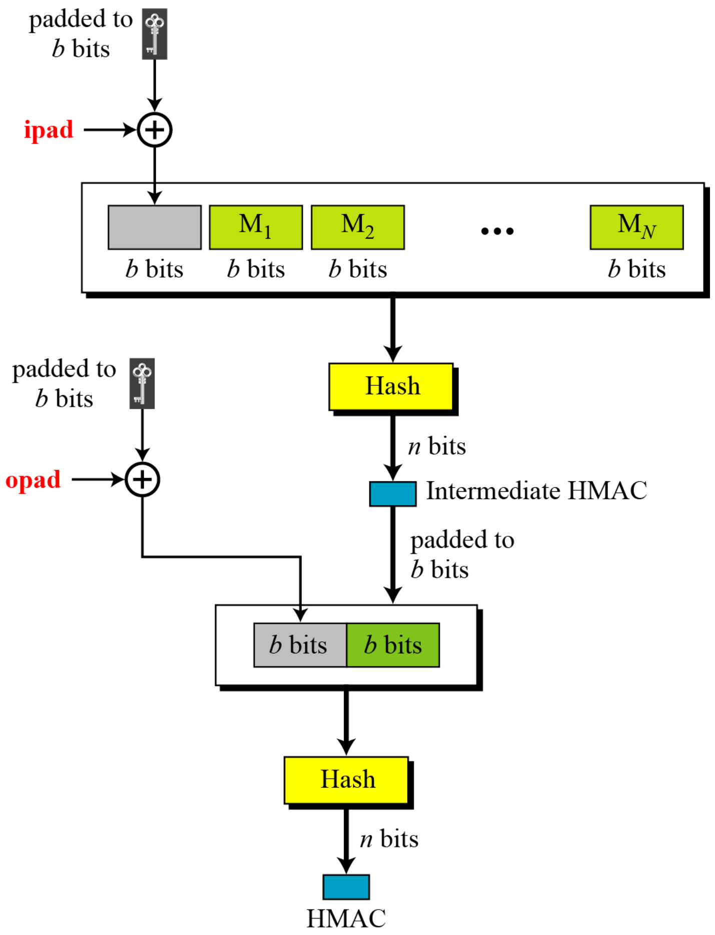
- Example:- tcpdump, wireshark
- Detection of clear-text passwords and usernames from the network.
- Conversion of data to human readable format so that people can read the traffic.
- Performance analysis to discover network bottlenecks.
- Troubleshoot network related problems
- Network intrusion detection in order to discover hackers.

Q.2 What is Hashed MAC (HMAC)? Explain with block diagram.

NIST (National Institute of Standards and Technology) has issued a standard (FIPS198) for a nested MAC

that is referred to as HMAC (hashed MAC).

1. The message is divided into *N* blocks, each of *b* bits.
2. The secret key is left-padded with 0's to create a *b*-bit key. Note that it is recommended that secret key (before padding) be longer than *n* bits, where *n* is the size of the HMAC.
3. The result of step 2 is XORed with a constant called ipad (input pad) to create a *b*-bit block. The value of ipad is the *b*/8 repetition of the sequence 00110110 ($(36)_{16}$).
4. The resulting block is prepended to *N*-block message.
5. The result is N+1 blocks.
6. 5. The result of step 4 is hashed to create an *n*-bit digest. We call the digest the *intermediate* HMAC.
7. 6. The intermediate *n*-bit HMAC is left padded with 0s to make a *b*-bit block.
8. 7. Step 2 and 3 are repeated by a different constant opad (output pad). The value of opad is the *b*/8 repetition of the sequence 01011100 ($(5C)_{16}$).
9. 8. The result of step 7 is prepended to the block of step
10. 9. The result of step 8 is hashed with the same hashing
11. algorithm to create the final *n*-bit HMAC.



Q.3. Explain Services of digital signature ?

1. Message Authentication

2. Message Integrity

3.Nonrepudiation

4.Confidentiality

Q.4. What are various Types of Malicious Code. Explain any two.

- Virus - program that attaches itself to non-malicious programs and propagates itself to other programs

- Trojan Horse – Malicious code that in addition to its primary non-malicious effect, has a non-obvious malicious effect

- Logic Bomb – only on a condition

- Time bomb – only at certain time

- Trapdoor (backdoor) – other means of privileged access; intentional and non-intentional . i.e. unauthorized acces to functionality
- Worm – spreads virus via network
- Rabbit – replicates to exhaust recourses
- Rootkits - Tools to misrepresent what is on the system
- Keylogger/spyware - Code that observers and reports actions on the computer

Q.5. Let A and B be the two entities communicating and let the prime number(p) be 11 as agreed upon by both. Using Diffie Hellman Key exchange, calculate the shared secret key if the random number chosen by A is 5 and that by B is 8.
Note : Find g .Show steps for calculation of the primitive root (g)

2^0 mod 11=1

2^1 mod 11=2

2^2 mod 11=4

2^3 mod 11=8

2^4 mod 11=5

2^5 mod 11=10

2^6 mod 11=9

2^7 mod 11=7

2^8 mod 11=3

2^9 mod 11=6

Hence

g=2

Let x=5   y=8

At A   R1= 2^5 mod 11=10

At B   R2= 2^8 mod 11=3

At A   3^5 mod 11 =1

At B   10^8 mod 11 = 1

Hence shared secret key = 1

Few Sample example of DH

Q. In a Diffie-Hellman Key Exchange, Alice and Bob have chosen prime value q = 353 and primitive root p = 3. If Alice’s secret key is 4 and Bob’s secret key is 6, what is the secret key they exchanged?

users Alice & Bob who wish to swap keys:

agree on prime q=353 and a or p=3

select random secret keys:

A chooses xA=97, B chooses xB=233

compute respective public keys:

yA=397 mod 353 = 40 (Alice)

yB=3233 mod 353 = 248 (Bob)

compute shared session key as:

KAB= yBxA mod 353 = = 160 (Alice)

KAB= yAxB mod 353 = = 160 (Bob)

OR

In a Diffie-Hellman Key Exchange, Alice and Bob have chosen prime value q = 17 and primitive root p = 5. If Alice’s secret key is 4 and Bob’s secret key is 6, what is the secret key they exchanged?

Given-

- n = 17
- a or p = 5
- Private key of Alice = 4
- Private key of Bob = 6

Step-01:

Both Alice and Bob calculate the value of their public key and exchange with each other.

Public key of Alice

= $5^{\text{private key of Alice}}$ mod 17

= 5^4 mod 17

= 13

Public key of Bob

= $5^{\text{private key of Bob}}$ mod 17

= 5^6 mod 17

= 2

Step-02:

Both the parties calculate the value of secret key at their respective side.

Secret key obtained by Alice

= $2^{\text{private key of Alice}}$ mod 7

= 2^4 mod 17

= 16

Secret key obtained by Bob

= $13^{\text{private key of Bob}}$ mod 7

= 13^6 mod 17

= 16

Finally, both the parties obtain the same value of secret key.

The value of common secret key = 16.