Cybersecurity Assignment 5

Name: Deep Ghadiyali

Roll Number: CS17B011

1. **Explain the main features of an a. application layer firewall b. packet filtering firewall.**
   a. An application-level firewall evaluates network packets for valid data at the application layer before allowing a connection. The firewall examines the data in all network packets at the application layer and maintains complete connection state and sequencing information. Other security items such as user password and service requests that appear in the application layer data can be validated by the firewall. Specialized application software and proxy services are included in most application layer firewalls. Proxy services manage traffic through a firewall for a specific service such as HTTP or FTP. Proxy services can provide increased access control, detailed checks for valid data, and generate audit records about the traffic they transfer because the proxy services are specific to the protocol that they are designed to forward. An application-level firewall analyses the complete command set for a single protocol in application space.
   b. A packet filter firewall analyses network traffic at the transport protocol layer. Each packet filter firewall analyses network traffic at the transport protocol layer. Each IP network packet is examined to see if it matches one of a set of rules defining what data flows are allowed. The rules determine whether communication is allowed based upon the information contained within the Internet and transport layer headers and the direction that the packet is headed. Packet filters enable the administrator to permit or prohibit the transfer of data based on the following controls: the physical network interface that the packet arrives on; the source IP address the data is coming from; the destination IP address the data is going to; the type of transport layer; the transport layer source port, and the transport layer destination port. The packet filter architecture performs an analysis for one or more network protocols using a very limited rule set. The packets coming into the trusted network are compared against defined rules composed from a limited rule set for one or more protocols such as IP, TCP, or ICMP. Packets are either accepted and passed to the network stack for delivery or are denied access.

`

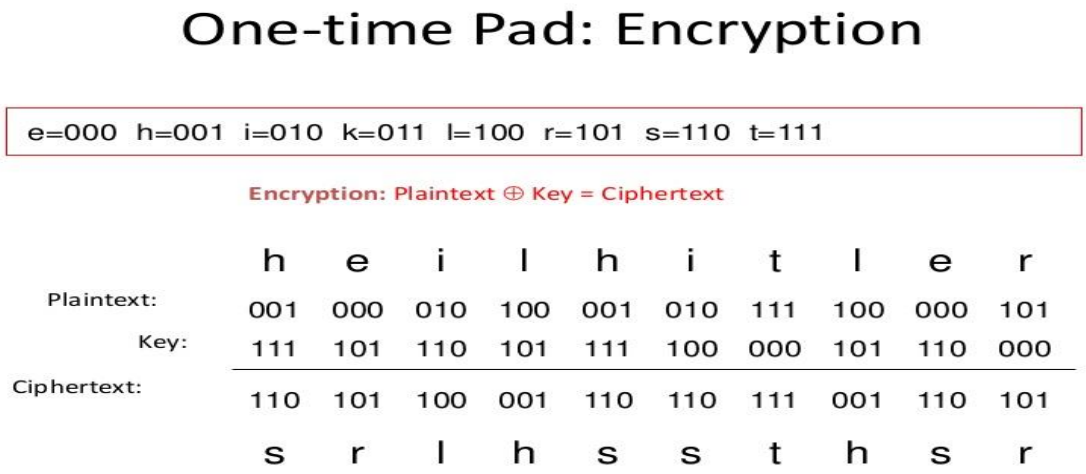
2. Give two examples of rules as applicable in SNORT

- *alert tcp any any -> 192.168.1.0/24 80 (content: "cgi-bin/phf"; offset: 3; depth: 22; msg: "CGI-PHF access";)*
- *alert tcp any any -> 192.168.1.0/24 21 (content: "USER root"; nocase; msg: "FTP root user access attempt";)*

3. Explain the process of encryption and decryption in One time pad with an example.

- *Encryption:*

  To encrypt a plaintext, a user needs to come up with a completely random key whose length is exactly same as the length of message. Then, each bit or character of the plaintext is encrypted by combining it with the corresponding bit or character from the key/pad using modular addition.



- *Decryption:*

  To decrypt a letter, user takes the key letter on the left and finds cipher text letter in that row. Here the key is subtracted from the ciphertext, again using modular arithmetic.

`

One-time Pad: Decryption

e=000 h=001 i=010 k=011 l=100 r=101 s=110 t=111

Decryption: Ciphertext ⊕ Key = Plaintext

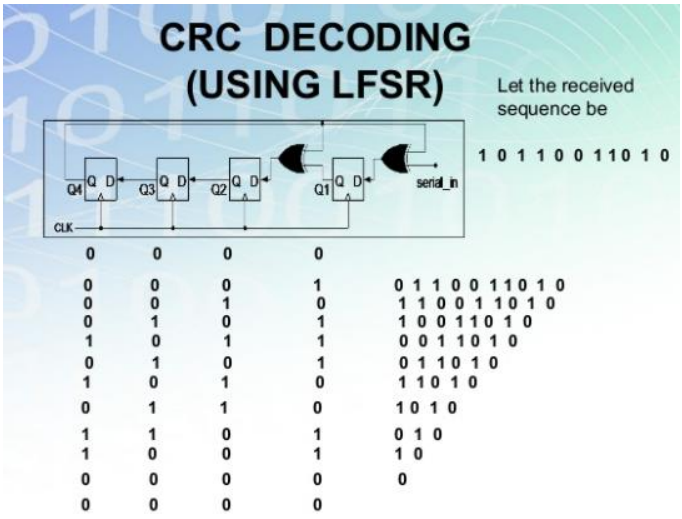
	s	r	l	h	s	s	t	h	s	r
Ciphertext:	110	101	100	001	110	110	111	001	110	101
Key:	111	101	110	101	111	100	000	101	110	000
Plaintext:	001	000	010	100	001	010	111	100	000	101
	h	e	i	l	h	i	t	l	e	r

4. Show an example of encryption and decryption with linear shift register with at least five bits.

Encryption:

```
01101000010
11010000101 1
10100001011 1
01000010110 0
10000101100 0
00001011001 1
00010110010 0
00101100100 0
01011001001 1
10110010010 0
01100100100 0
```

Decryption:



5. Show the functionality of at least two digital forensics tools. What kind of data do they analyse?

- *Autopsy:*
  Autopsy is a digital forensics platform and graphical interface to The Sleuth Kit and other digital forensics tools which displays the results from the forensic search of the underlying volume making it easier for investigators to flag pertinent sections of data. Autopsy analyses major file systems (NTFS, FAT, ExFAT, HFS+, Ext2/Ext3/Ext4, YAFFS2) by hashing all files, unpacking standard archives (ZIP, JAR etc.), extracting any EXIF values and putting keywords in an index. Some file types like standard email formats or contact files are also parsed and cataloged.

- *Network Miner:*
  Network Miner is an open-source Network Forensic Analysis Tool (NFAT) for Windows (but also works in Linux / Mac OS X / FreeBSD). Network Miner can be used as a passive network sniffer/packet capturing tool in order to detect operating systems, sessions, hostnames, open ports etc. without putting any traffic on the network. Network Miner can also parse PCAP files for off-line analysis and to regenerate/reassemble transmitted files and certificates from PCAP files.
  Network Miner makes it easy to perform advanced Network Traffic Analysis (NTA) by providing extracted artifacts in an intuitive user interface. The way data is presented not only makes the analysis simpler, it also saves valuable time for the analyst or forensic investigator.

6. Explain vignere encryption and decryption with an example

- *Encryption:*
  Along with the plaintext, the Vigenère cipher also requires a key, which is repeated so that the total length is equal to that of the plaintext.
  To encrypt, pick a letter in the plaintext and its corresponding letter in the key, use the key letter and the plaintext letter as the row index and column index, respectively, and the entry at the row-column intersection in the 26×26 Vigenère table with A to Z as the row heading and column heading is the letter in the ciphertext.

  Example:

`

```
Original Text:  CYBERSECURITYTEST
Key:            TESTKEY
Ciphertext:     VCTXBWCVYJBDCRXWL
```

- *Decryption:*

  To decrypt, pick a letter in the ciphertext and its corresponding letter in the key, use the key letter to find the corresponding row, and the letter heading of the column that contains the ciphertext letter is the needed plaintext letter.

  Example:

```
Ciphertext:     VCTXBWCVYJBDCRXWL
Key:            TESTKEY
Decrypted Text: CYBERSECURITYTEST
```

`