Network Threats

6COSC019W- Cyber Security

Dr Ayman El Hajjar

February 06, 2024

School of Computer Science and Engineering
University of Westminster

OUTLINE

1. Sniffers
2. Application layer attacks
    - HTTP
        - DNS
    - Session layer attacks
    - Transport layer attacks
3. Network layer attacks
4. Data Link layer attacks
5. Denial of Service attacks

MALICIOUS ACTIVITY ON THE RISE

- ❏ Examples of the malicious attacks are everywhere
- ❏ Data breaches occur in both public and private sectors
- ❏ In 2020, China was top country of origin for cyberattacks, at 41 percent.
- ❏ United States was second at 10 percent.
- ❏ Real time attacks maps below:
    - ❐ DDoS real time attacks
    - ❐ Cyberthreats real time map
    - ❐ Cyberthreats real time map

Sniffers

❏ An application or device designed to capture, or “sniff, network traffic as it moves across the network

❏ A technology used to steal or observe information

❏ Allows viewing of email passwords, web passwords, File Transfer Protocol (FTP) credentials, email contents, and transferred files

❏ When a network adapter is put in promiscuous mode **(also called monitor mode)**, a sniffer then realise its full potential, including sniffing all traffic regardless of the destination address.

> In normal mode the network adaptor drops or ignores any packet not intended for it
>
> In promiscuous mode the network adaptor captures all traffic it can hear.

Sniffers Threats to protocols

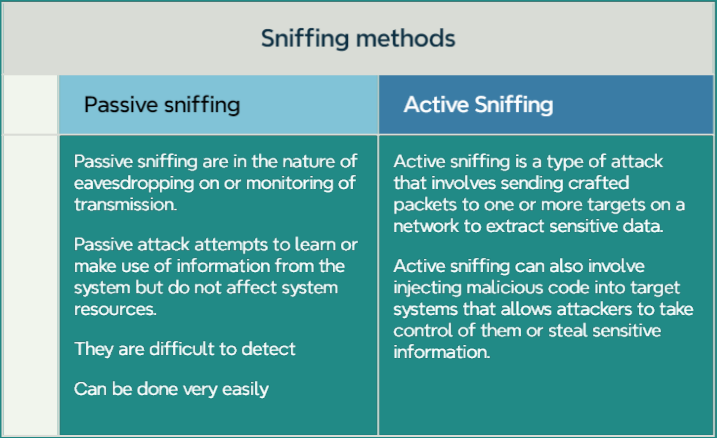
❒ Telnet Keystrokes can be easily sniffed if transmitted over Telnet

❒ Hypertext Transfer Protocol (HTTP) Designed to send information in the clear without any protection and is a good target for sniffing

❒ Simple Mail Transfer Protocol (SMTP) Commonly used in the transfer of email; is simple and efficient but does not include protection against sniffing

❒ Post Office Protocol (POP) Is designed to retrieve email from servers but does not include protection against sniffing because passwords and usernames can be intercepted

❒ File Transfer Protocol (FTP) A protocol designed to send and receive files; all transmissions are sent in the clear



Sniffing methods

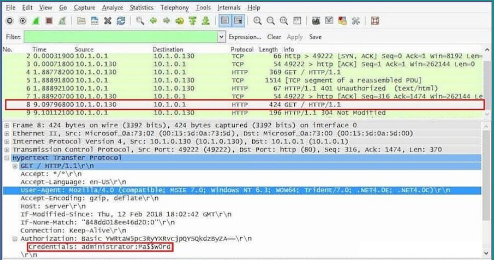
	Passive sniffing	Active Sniffing
	Passive sniffing are in the nature of eavesdropping on or monitoring of transmission. Passive attack attempts to learn or make use of information from the system but do not affect system resources. They are difficult to detect Can be done very easily	Active sniffing is a type of attack that involves sending crafted packets to one or more targets on a network to extract sensitive data. Active sniffing can also involve injecting malicious code into target systems that allows attackers to take control of them or steal sensitive information.

Application layer attacks

Passive Attacks- HTTP basic authentication

- ❑ Example of such attacks is the HTTP authentication:
  - ❑ HTTP basic authentication is a simple challenge and response mechanism with which a server can request authentication information (a user ID and password) from a client.

    The client passes the authentication information to the server in an Authorization header.
  - ❑ Insecure as full credentials pass over the wire and are sent in the clear

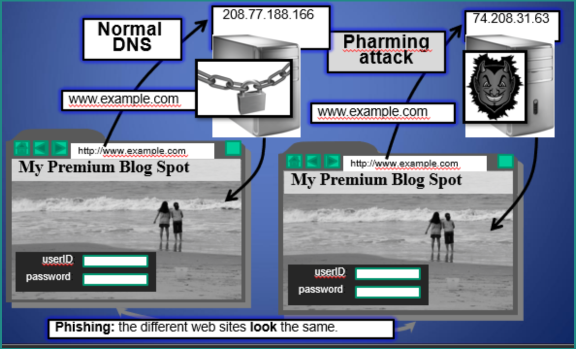

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.  Time        Source      Destination  Protocol Length Info
   2 0.00031900 10.1.0.1    10.1.0.130   TCP        66 http > 49222 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=
   3 0.00071800 10.1.0.130  10.1.0.1     TCP        54 49222 > http [ACK] Seq=1 Ack=1 Win=262144 Len=0
   4 1.88778200 10.1.0.130  10.1.0.1     HTTP      369 GET / HTTP/1.1
   5 1.88891800 10.1.0.1    10.1.0.130   TCP      1514 [TCP segment of a reassembled PDU]
   6 1.88892100 10.1.0.1    10.1.0.130   HTTP       67 HTTP/1.1 401 Unauthorized  (text/html)
   7 1.88920700 10.1.0.130  10.1.0.1     TCP        54 49222 > http [ACK] Seq=316 Ack=1474 Win=262144 Le
   8 9.09796800 10.1.0.130  10.1.0.1     HTTP      424 GET / HTTP/1.1
   9 9.10112100 10.1.0.1    10.1.0.130   HTTP      196 HTTP/1.1 304 Not Modified

⊞ Frame 8: 424 bytes on wire (3392 bits), 424 bytes captured (3392 bits) on interface 0
⊞ Ethernet II, Src: Microsof_0a:73:02 (00:15:5d:0a:73:5d), Dst: Microsof_0a:73:00 (00:15:5d:0a:5d:00)
⊞ Internet Protocol Version 4, Src: 10.1.0.130 (10.1.0.130), Dst: 10.1.0.1 (10.1.0.1)
⊞ Transmission Control Protocol, Src Port: 49222 (49222), Dst Port: http (80), Seq: 316, Ack: 1474, Len: 370
⊟ Hypertext Transfer Protocol
  ⊞ GET / HTTP/1.1\r\n
    Accept: */*\r\n
    Accept-Language: en-US\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.3; WOW64; Trident/7.0; .NET4.0E; .NET4.0C)\r\n
    Accept-Encoding: gzip, deflate\r\n
    Host: server\r\n
    If-Modified-Since: Thu, 12 Feb 2018 18:02:42 GMT\r\n
    If-None-Match: "848dd018ee46d20:0"\r\n
    Connection: Keep-Alive\r\n
  ⊟ Authorization: Basic YWRtaW5pc3RyYXRvcjpQYSQkdzByZA==\r\n
      Credentials: administrator:Pa$$w0rd
    \r\n
```

DNS attacks- DNS Pharming

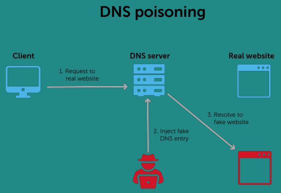
❑ An attacker attempt to change the IP associated with a server maliciously:



DNS attacks- DNS cache poisoning

- ❑ **Basic idea:** Give DNS servers false records and get it cached
- ❑ There are 3 main different ways to do DNS cache poisoning.
  - ❒ The first relies on redirecting the nameserver of the attacker's domain to the nameserver of the target domain, and then assigning this target nameserver a fake IP address.
  - ❒ The second variant relies on redirecting the nameserver of another, unrelated domain to a fake nameserver.
  - ❒ The third variant just involves "racing" the real nameserver to give

- ❑ Cache may be poisoned when a nam server:
  - Disregards identifiers
  - Has predictable ids
  - Accepts unsolicited DNS records



Session Hijacking

❏ Session hijacking builds on sniffing the network.

❏ The goal is not only to observe traffic and sessions currently active on the network but also to take over a session that has authenticated access to the resource

❏ Occurs when attackers use a valid session to gain unauthorised access to a system, information, or service

❏ Target authentication, which typically takes place at the beginning of a session, making session hijacking possible after that point

❏ Relies on a basic understanding of how messages and their packets flow over the Internet

Session Hijacking (Cont.)

❏ In a session hijacking attack, an attacker takes control of or modifies any communications between two hosts by:

- ❒ placing themselves between Party A and Party B.
- ❒ Monitor the flow of packets using sniffing techniques.
- ❒ Analyse and predict the sequence number of the packets.
- ❒ Sever the connection between the two parties.
- ❒ Seize control of the session.
- ❒ Perform packet injection into the network.

IDENTIFYING AN ACTIVE SESSION

❏ For a session hijack to be successful, attacker must locate and identify a suitable session for hijacking

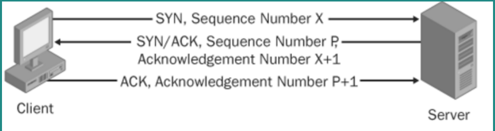
❏ An attacker must successfully determine or guess the sequence numbers to hijack a session.

Sequence number prediction:

❏ When a client transmits a SYN packet to a server, the response will be a SYN/ACK. The client then responds to this SYN/ACK with an ACK. During this handshake, the starting sequence number will be assigned using a random method if the operating system supports this function.

❏ If this sequence number is predictable, the attacker can initiate the connection to the server with a legitimate address and then open up a second connection from a forged address.

AN EXAMPLE- HIJACKING A TCP SESSION


SYN, Sequence Number X
SYN/ACK, Sequence Number P,
Acknowledgement Number X+1
ACK, Acknowledgement Number P+1
Client
Server

- **Enter the attacker**:
  - Spoof the client’s IP address: Easy
  - Determine the correct sequence number the server is expecting from the client. Nothing a good network sniffer can’t figure out.
  - Inject data into the session before the client sends its next packet.
  - **Note:** The attacker needs a way to ”hold down” the client from sending into the session new data that would shift sequence numbers forward (DoS) client or send before.

Session Hijacking (Cont.)

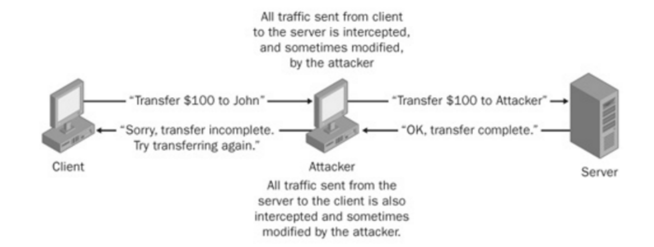
- ❑ Session hijacking takes advantage of the fact that most communications are protected from the beginning at session setup, such as by providing credentials, but not during the session.
- ❑ Session hijacking attacks generally fall into the following three categories:
  - ❒ Man in the middle attack
  - ❒ Blind hijack attacks
  - ❒ Session theft attacks

MAN IN THE MIDDLE ATTACK (MITM)

❑ An attacker intercepts all communications between two hosts.

❑ The attacker positions themselves so that communications between a client and server must flow through them, which allows them to modify the communications.

❑ Protocols that rely on the exchange of public keys to protect communications, for example, are often the target of these types of attacks (ARP, DNS)


All traffic sent from client to the server is intercepted, and sometimes modified, by the attacker
"Transfer $100 to John"
"Transfer $100 to Attacker"
"Sorry, transfer incomplete. Try transferring again."
"OK, transfer complete."
Client
Attacker
Server
All traffic sent from the server to the client is also intercepted and sometimes modified by the attacker.

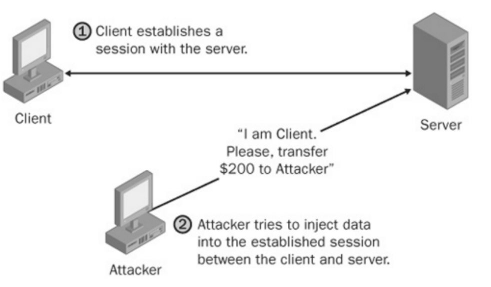
BLIND HIJACK ATTACK

❑ An attacker can inject data such as malicious commands into those communications

❑ This type of attack is called blind hijacking because the attacker can only inject data into the communications stream;

❑ The attacker cannot see the response to that data, such as ”The command completed successfully.

❑ This method of hijacking is still very effective.


① Client establishes a session with the server.
Client
Server
“I am Client. Please, transfer $200 to Attacker”
② Attacker tries to inject data into the established session between the client and server.
Attacker

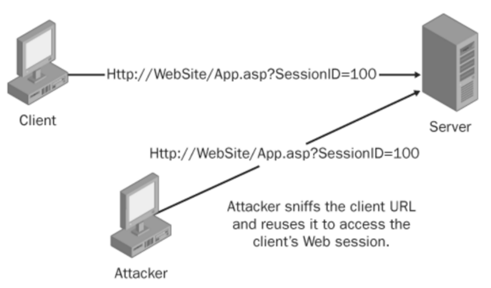
Session replay attack

❑ In a session replay attack also called session theft attack, the attacker is neither intercepting nor injecting data into existing communications between two hosts.

❑ Instead, the attacker creates new sessions or utilizes old sessions.

❑ Repeat sessions !!

❑ This type of session hijacking attack is most common at the application level, such as a Web application.


Http://WebSite/App.asp?SessionID=100
Client
Server
Http://WebSite/App.asp?SessionID=100
Attacker sniffs the client URL and reuses it to access the client's Web session.
Attacker

PORT SCANNING

❑ Port scanning is an essential step in the reconnaissance phase. Several scans exist, each reveals different type of information:

❒ **Ping Scan**: The ping scan sends a single ICMP echo request from the source to the destination device. A response from an active device returns an ICMP echo reply, unless the IP address is not available on the network or the ICMP protocol is filtered.

❒ **Connect scan:** Fully connect to the target ip address and port in a complete TCP handshake. Reliable but very noisy.

❒ **SYN Scan:** also called half open, sends SYN requests to the target to gather information about open ports without completing the TCP handshake. When an open port is identified, the TCP handshake is reset before it can be completed.

FIN Scan: Sends a FIN (or finish) packet to target. If that port is not listening, no response. If it is listening an error response is received.

PORT KNOCKING

❑ Port knocking is the act of attempting to make connections to blocked ports in a certain order in an attempt to open a port

❑ Port knocking however is very susceptible to replay attacks. Someone can theoretically record port knocking attempts and repeat those to get the same open port again

❑ Port knocking is fairly secure against brute force attacks since there are 65536k combinations, where k is the number of ports knocked

❑ One good way of protecting against replay attacks would be a time dependent knock sequence.

Network layer attacks

IP Vulnerabilities

- Unencrypted transmission
  - **Eavesdropping** possible at any intermediate host during routing
- No source authentication
  - Sender can **spoof source address**, making it difficult to trace packet back to attacker
- No integrity checking
  - Entire packet, header and payload, can be modified en route to destination, enabling **content forgeries**, **redirections**, and **man-in-the-middle** attacks
- No bandwidth constraints
  - Large number of packets can be injected into network to launch a **denial-of-service** attack

IP SPOOFING ATTACKS

- ❒ IP Spoofing is an attempt by an intruder to send packets from one IP address that appear to originate at another
- ❒ If the server thinks it is receiving messages from the real source after authenticating a session, it could inadvertently behave maliciously
- ❒ There are two basic forms of IP Spoofing
  - ❒ Blind Spoofing
    - ❒ Spoof IP address without inherently knowing the ACK sequence pattern.
  - ❒ Non-Blind Spoofing
    - ❒ Spoof IP address after identifying correct ACK sequence.

IP SPOOFING ATTACKS

❏ For both to succeed, the spoofed IP cannot exist with another user on the network.

✦ **Remember**: Two devices with the same IP connect exist on a network. For this attack to be successful, the spoofed IP cannot exist on the network. For Non blind IP spoofing, the attacker usually conduct a Denial of Service attack on the genuine client rendering them unavailable.

❏ For Non Blind spoofing, the attacker would:

- ❐ Analyse the network packets using a packet sniffer,
- ❐ Determine the ACK sequence pattern
- ❐ Spoof the IP of an actual client and send packets with the correct sequenced acknowledgment number

Data Link layer attacks

MAC Flooding

❑ The goal of MAC flooding is to flood the switch with fake MAC addresses to all ports.

❑ This will cause the switch Content Addressable memory (CAM) to be filled and the switch overwhelmed. This will result in the switch failing.

- ❒ Content Addressable memory (CAM) is used to build a lookup table
- ❑ Lookup table tracks which MAC addresses are present on which ports on the switch
- ❑ CAM allows a lookup to be performed to let the switch get traffic to the correct port and host

MAC Flooding

MAC flooding is considered an active sniffing attack.

MAC Filtering and MAC Spoofing

MAC Filtering

The network administrator can create a **block** or **allow** lists of MAC addresses to certain network. This is called MAC Filtering.

❐ For example Wireless Networks use MAC filtering to only allow certain devices to connect to the network.

❑ A MAC spoofing attack impersonates another machine

❑ Find out MAC address of target machine using a packet sniffer

❑ Reconfigure MAC address of rogue machine

❑ Turn off or unplug target machine

❐ Going back to the Wireless Networks example, and although it is meant to be a security control, it is very easy to spoof the MAC address making this control ineffective.

ARP SPOOFING

- ❑ The ARP table is updated whenever an ARP response is received
- ❑ Requests are not tracked
- ❑ ARP announcements are not authenticated
- ❑ Machines trust each other
- ❑ A rogue machine can spoof other machines

ARP Poisoning

❑ A method of bypassing a switch where sniffing is performed on an IPv4 network

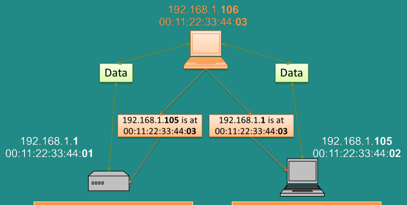
❑ The basic idea of ARP poisoning is for the attacker to attach itself to a network with a valid IP address and a spoofed MAC address from the switch ARP table stored in the CAM.

❑ ARP poisoning is considered an active sniffing attack on IPv4 networks.

❑ An arp cache updates every time that it receives an arp reply! Even if it did not send any arp request!

❑ The attacker first need to stop the client from sending into the session new data

❑ To do this, the attacker could just send the data to inject and hope it is received before the real client can send new data or Dos the Client



192.168.1.**106**
00:11:22:33:44:**03**

Data

Data

192.168.1.**105** is at
00:11:22:33:44:**03**

192.168.1.**1** is at
00:11:22:33:44:**03**

192.168.1.**1**
00:11:22:33:44:**01**

192.168.1.**105**
00:11:22:33:44:**02**

Denial of Service attacks

Denial-of-Service Attacks

Denial-of-Service Attacks

❑ One of the most common types of attacks. It prevents legitimate users from accessing the system

❑ Intended to prevent services from being delivered

❑ A form of attack on the availability of some service

❑ Are frequently aimed to consume resources, but may also involve actual disruption of a service or server. The idea is that computers have physical limitations

- ❒ Number of users
- ❒ Size of files
- ❒ Speed of transmission
- ❒ Amount of data stored

❑ Another type of DoS attacks aims to exploit programming defects causing them to crash

DISTRIBUTED DENIAL OF SERVICE ATTACKS

❏ A DoS attack attempts to prevent valid users from accessing network resources.

❏ A distributed denial of service (DDoS) attack has the same goal but amplifies the DoS attack by using multiple hosts.

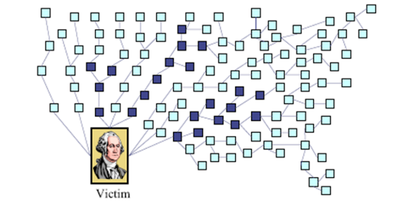
❏ Whereas a DoS attack would overwhelm the network connection for a targeted host through a more powerful host, a DDoS attack would use multiple intermediary hosts to generate enough traffic to disrupt server farms or a whole network segment, and possibly beyond.

❏ A challenge to detect a DDos is that traffic is coming from several ip addresses. That makes it more difficult to detect until it is too late

Distributed Denial of Service Attack

- ❑ Uses hundreds or thousands of systems to conduct attack
- ❑ Has primary and secondary victims
- ❑ Attack can be difficult or impossible to track back to source
- ❑ Defence is difficult, and impact is higher than DoS attack, due to number of attackers

DDoS



DoS/DDoS Attacks: Exploitation of Programming Defects

- ❑ The Ping of Death (PoD)
  - ❒ Some systems cannot handle oversized packets; .
  - ❒ An attacker sends them out in fragments, when fragments reach the system, they are reassembled by the victim;
  - ❒ When the maximum size (65,536 bytes) allowed by the IP protocol is reached, some systems will crash
- ❑ Teardrop Attack
  - ❒ Packets are sent in a malformed state with their offset values adjusted so they overlap, which is illegal;
  - ❒ Victim system attempts to reconstruct message. when a system that does not know how to deal with this issue is targeted, a crash or lock may result
- ❑ Land Dos
  - ❒A packet is sent to a victim's system with the same source and destination address and port; systems that do not know how to process this will crash

DoS/DDoS Attacks: Consumption of Resources

- ❑ SYN flood
  - ❒ Uses forged packets with the SYN flag set;
  - ❒ when the victim receives enough of the packets, the result is an overwhelmed system as the SYN flood consumes connection resources to the point where no resources are available for legitimate connections
- ❑ ICMP flood
  - ❒ Comes in two variants: Smurf attack and ping flood
- ❒ Smurf attack
  - ❒ Carried out when a large amount of traffic is directed to the broadcast address of a network instead of to a specific system; because the attacker configures the packet with the intended victim as the source, all hosts on the network respond to the victim instead of to the attack

DoS/DDoS Attacks: Consumption of Resources (Cont.)

Ping flood

- ❒ Carried out by sending a large number of ping packets to the victim with the intent of overwhelming the victim; very simple attack

❒ Reflected attack

- ❒ Is carried out by spoofing or forging the source address of packets or requests and sending them to numerous systems, which in turn respond to the request; a scaled-up version of what happens in the ping flood attack

❒ DHCP starvation

- ❒ If enough requests flooded onto the network, the attacker can completely exhaust the address space allocated by the DHCP servers for an indefinite period of time. This is a DoS attack is called DHCP starvation. There are An attacker can use a tools such as The Gobbler that will do this for the attacker to easily commit this type of attack.

DoS/DDoS Attacks: Consumption of Resources (Cont.)

HTTP flood

- ❒ Attack that bombards Web servers with HTTP requests
- ❒ Consumes considerable resources

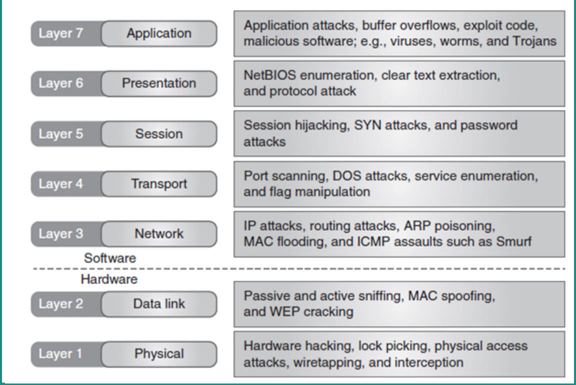
❒ Slowloris A more potent variant

- ❒ Attempts to monopolize by sending HTTP requests that never complete
- ❒ Eventually consumes Web server's connection capacity
- ❒ Utilises legitimate HTTP traffic

BOTNETS AND THE INTERNET OF THINGS (IOT)

- ❑ Botnets
  - ❒ Consist of computers and devices (Mainly Internet of Things devices) that are infected with software such as those used in DDoS attacks
  - ❒ Can stretch across globe
- ❑ Botnets attacks include:
  - ❒ DDoS attacks This construct makes sense as an attack method based on the way a DDoS works and the number of systems that can be infected.
  - ❒ Click fraud This attack is where the attackers infect a large number of systems with the idea that they will use the infected systems to click on ads on their behalf, generating revenue for themselves.
  - ❒ Stealing information Attacks have also been carried out with botnets to steal information from unsuspecting users' systems.

Mapping the OSI Model to Cyber Threats



Layer 7	Application	Application attacks, buffer overflows, exploit code, malicious software; e.g., viruses, worms, and Trojans
Layer 6	Presentation	NetBIOS enumeration, clear text extraction, and protocol attack
Layer 5	Session	Session hijacking, SYN attacks, and password attacks
Layer 4	Transport	Port scanning, DOS attacks, service enumeration, and flag manipulation
Layer 3	Network	IP attacks, routing attacks, ARP poisoning, MAC flooding, and ICMP assaults such as Smurf
Software		
Hardware		
Layer 2	Data link	Passive and active sniffing, MAC spoofing, and WEP cracking
Layer 1	Physical	Hardware hacking, lock picking, physical access attacks, wiretapping, and interception

REFERENCES

❑ The lecture notes and contents were compiled from my own notes and from various sources.

❑ Figures and tables are from the recommended books

❑ **The lecture notes are very detailed. If you attend the lecture, you should be able to understand the topics.**

❑ **You can use any of the recommended readings! You do not need to read all the chapters!**

❑ **Recommended Readings note:** Focus on what was covered in the class.

- ❒ Chapter 2- Networking Foundations, CEH v11 Certified Ethical Hacker Study Guide
- ❒ Chapter 5, Network and telecommunications, Fundamentals of Information Systems Security
- ❒ Chapter 19 Introduction, CyBOK, The Cyber Security Body of Knowledge