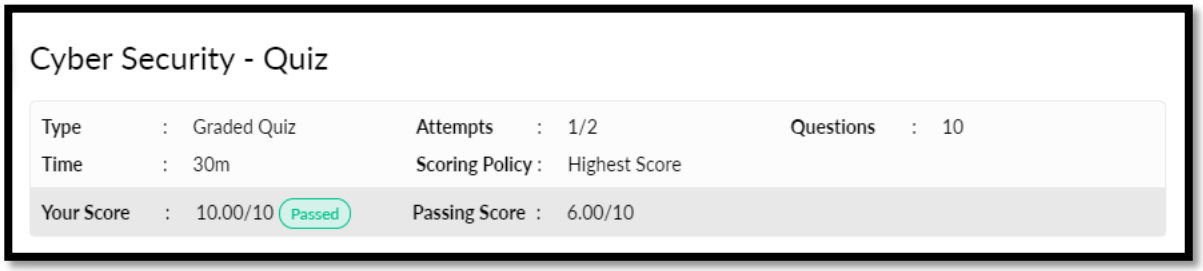
DAILY ASSESSMENT

Date:	**19/06/2020**	**Name:**	**Davis S. Patel**
Course:	**Cyber Security**	**USN:**	**4AL16EC045**
Topic:	**Course QUIZ**	**Semester & Section:**	**8th - A**
GitHub Repository:	**Davis**		

FORENOON SESSION DETAILS

Image of session

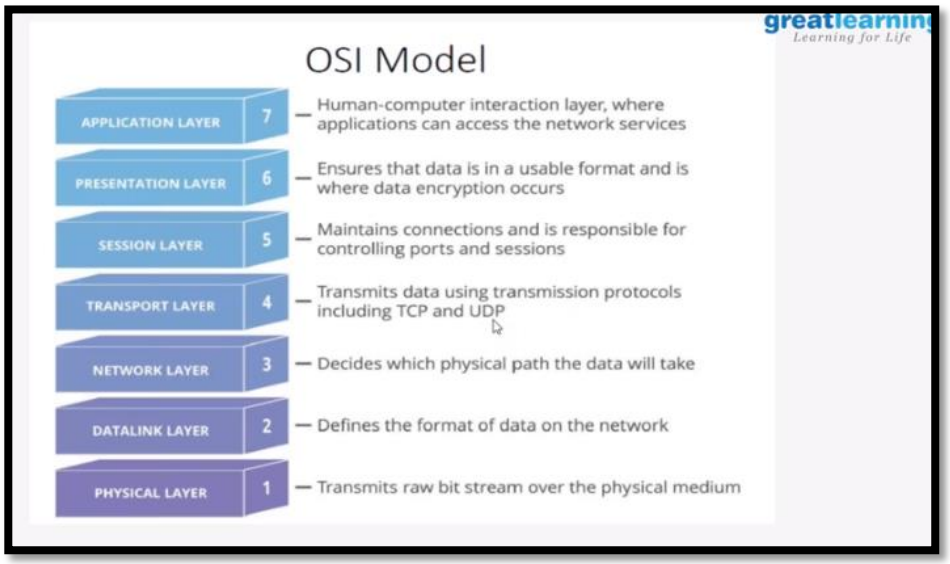


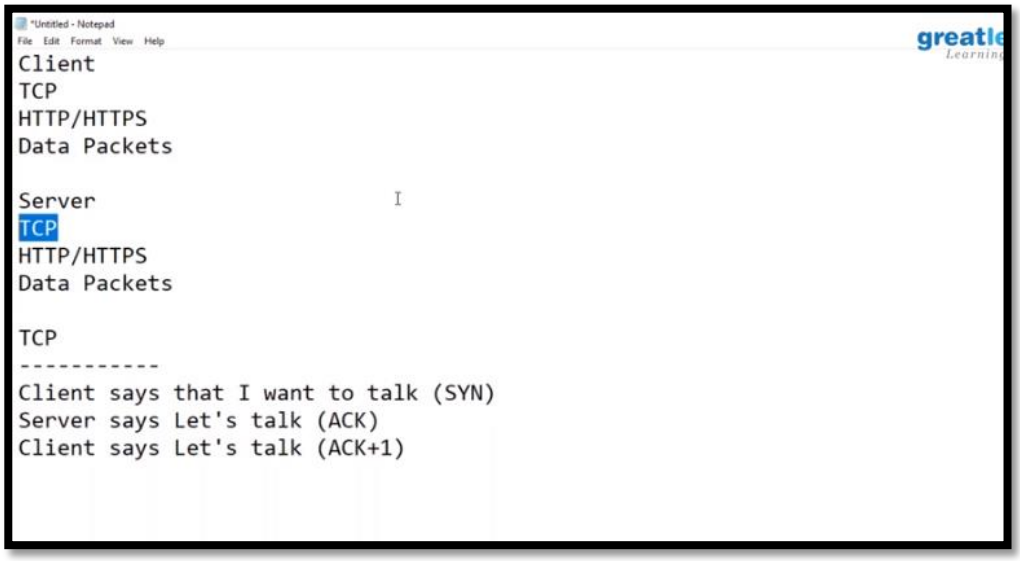
DAILY ASSESSMENT

Date:	**19/06/2020**	**Name:**	**Davis S. Patel**
Course:	**Ethical Hacking**	**USN:**	**4AL16EC045**
Topic:	**Ethical hacking in web applications – Demonstration Ethical hacking in network architecture -Demonstration**	**Semester & Section:**	**8th - A**
GitHub Repository:	**Davis**		

AFTERNOON SESSION DETAILS

Image of Session


greatlearning
Learning for Life
OSI Model
APPLICATION LAYER 7 — Human-computer interaction layer, where applications can access the network services
PRESENTATION LAYER 6 — Ensures that data is in a usable format and is where data encryption occurs
SESSION LAYER 5 — Maintains connections and is responsible for controlling ports and sessions
TRANSPORT LAYER 4 — Transmits data using transmission protocols including TCP and UDP
NETWORK LAYER 3 — Decides which physical path the data will take
DATALINK LAYER 2 — Defines the format of data on the network
PHYSICAL LAYER 1 — Transmits raw bit stream over the physical medium


*Untitled - Notepad
File Edit Format View Help
Client
TCP
HTTP/HTTPS
Data Packets
Server
TCP
HTTP/HTTPS
Data Packets
TCP

Client says that I want to talk (SYN)
Server says Let's talk (ACK)
Client says Let's talk (ACK+1)

REPORT –

Computer hacking is a practice with many nuances. Intent, whether benign or malicious, is often in the eyes of the beholder. When examining the root cause of a website hack or application exploit, it pays to follow the money. A hacker will be motivated by whomever or whatever is sponsoring his or her actions. The computer security industry coined the term “ethical hacking” to describe a hacker who benevolently attacks a network or other security system – whether private or public – on behalf of its owners. Ethical hackers are also called white hat hackers, as distinguished from the black-hatted bad guys.

One grey area in ethical hacking is hacktivism, where the hacker detects and reports (but sometimes exploits) security vulnerabilities as a form of social activism. In these cases, the motivation isn’t money, but rather to call attention to an issue or injustice the hacker believes merits social change. However, the victim of the hack may not be so receptive to this message. Ethical hacking should always be undertaken with the express advance consent of the targeted organization – as many black hat hackers claim to be ethical hackers when caught.

Simply put, a web application is any application that is accessed via a web browser. The browser is the client that runs the web application and allows the user to enter information. The server is the Internet or intranet which stores and retrieves information for all user clients. Information is generated dynamically by the web application through a web server and sent to user browsers. Many of today’s websites are essentially large web applications themselves. One common and prevalent example of a web application is web-based email services such as Gmail or Yahoo.

Web applications are popular because of the ubiquity of the Internet. Prior to the web, developers needed to build separate clients for specific computer operating systems – such as Apple, PC or Unix. Now users can access web applications regardless of OS or browser type; however some may run better in

specific browsers. This cross-platform compatibility explains their popularity as an application development model – web apps can be deployed and maintained easily without needing to update client-side software. Increases in broadband access and processing power have only improved performance, even when accessed by smartphone.

Web application development employs both client-side script (e.g. HTML, JavaScript) to store and retrieve information and server-side script (e.g. ASP, PHP) to present information. There is wide variation across web applications in the balance of client-side functionality to server-side functionality. Some are simply online storage applications with all tasks completed on the user side; while others offer complete online office suites with robust server processing. Regardless of the mix, if a browser is the common user interface – it's a web application.

Web application security practice now extends to web services and websites themselves. The internet is inherently insecure. Users and developers of web applications alike need to consider application security.

Most web applications are custom-made and, it must be assumed, have been subjected to a lesser degree of testing than off-the-shelf software. Users must keep their browser of choice up-to-date to patch any new security holes. They should carefully consider how a web application may access local storage or other sensitive information on their device. They should think twice before using file sharing, collaboration features, online payment, notifications and other permission-based functionality.

Likewise, developers must build trust and assurance with users of their web applications. These apps can theoretically track anything that users do, leading to privacy concerns. Forcing updated browser compatibility is one way to enforce application security, but this risks alienating large numbers of current users in the process. Securing personal information stored in databases is another, but ignores the fact that most hacks and attacks enter via the

application. If the web application is not secure, then sensitive user information remains at serious risk.

The best method (and the one most in the application developer's control) is to secure web applications from the inside by avoiding common coding errors that make web software vulnerable. Web application testing during the development process can expose cross-site scripting, SQL injection and other common security flaws. Vera code offers web application developers a host of web scanning, black box, white box, and manual penetration testing services to find and remediate these problems.

While a network security firewall is a critical piece of security technology, hardware or software firewalls on their own aren't enough to fully protect your organization or improve data security.

The network security firewall provides defenses against potential cyberattacks by inspecting packets of information as they enter the network or transfer between computers. When the content of a packet matches certain filter rules, the network security firewall can block the packet and send an error response.

Network security firewall technology has evolved in significant ways in recent years. While the original network security firewall examined traffic only at the network layer, more recent firewalls examine the transport layer as well. The latest network security firewall technology operates at the application layer to block unauthorized processes that could lead to the spread of malware software like malicious worms and viruses.

For this reason, the network security firewall remains an important line of defense, but it's not enough to stop all threats. Firewall technology tends to examine packets for known patterns, and emerging threats may be able to slip by unnoticed. For this reason, network and data security practices should include application security testing in order to defend the organization against an evolving universe of threats.