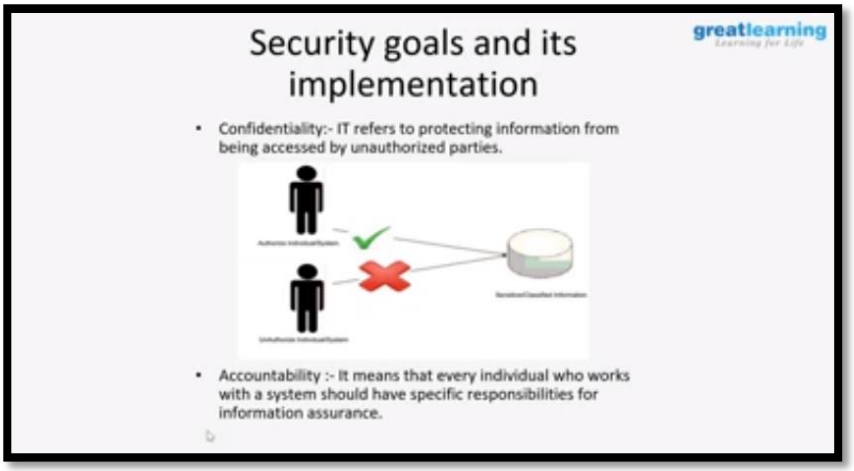
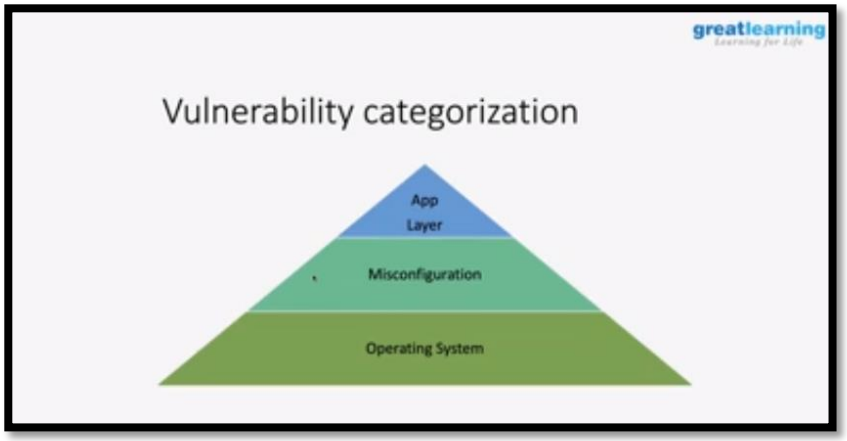
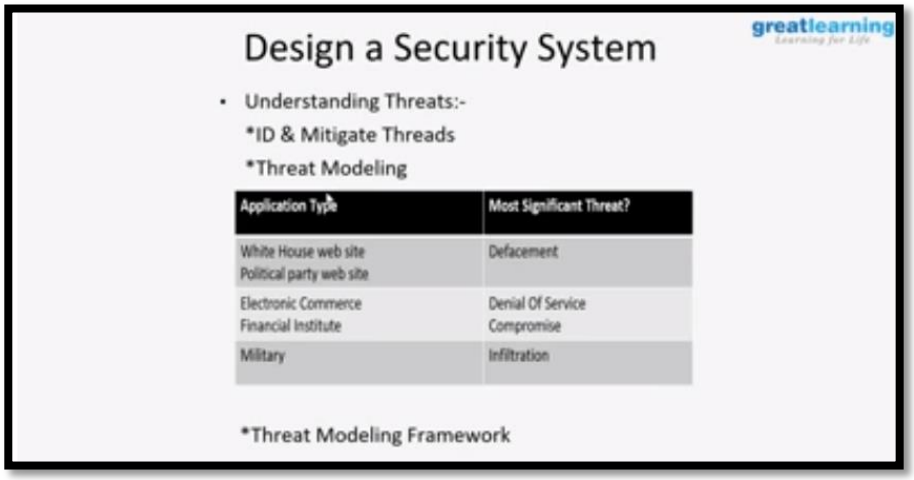
DAILY ASSESSMENT

Date:	**18/06/2020**	**Name:**	**Davis S. Patel**
Course:	**Cyber Security**	**USN:**	**4AL16EC045**
Topic:	**What is cyber security and what is the motivation behind it? Secure system design and security goals Threats Vulnerabilities & Password Security**	**Semester & Section:**	**8th - A**
GitHub Repository:	**Davis**		

FORENOON SESSION DETAILS
Image of session







REPORT –

To be useful, systems very often need to move, store and provide access to sensitive data. Unfortunately, this makes them prime targets for cyber-attack. If these systems are successfully compromised, the fallout can be damaging, expensive and embarrassing.

However, the picture need not be a bleak one. Frequently, the very worst outcomes can be avoided if services are designed and operated with security as a core consideration. With this in mind we have developed a set of principles to guide you in the creation of systems which are resilient to attack, but also easier to manage and update.

Throughout this guidance, we use the term system, by which we mean 'a collection of digital components that are connected using communication technologies to perform a business function.' A good example of the sort of system we are describing here is the UK's online passport application service, but it could refer to many other digitally-enabled business functions.

We will also use the term cyber-physical system, by which we mean 'a system that measures or controls the physical world to achieve a particular goal.' A good example is a modern car, in which complex logic measures the physical environment in order to control the movement of the vehicle.

Cyber threats are security incidents or circumstances with the potential to have a negative outcome to your network or other data management systems. Examples of common types of security threats include phishing attacks that result in the installation of malware that infects your data, failure of a staff member to follow data protection protocols that causes a data breach or even a tornado that takes down your company's data headquarters, disrupting access.

Vulnerabilities are the gaps or weaknesses in a system that make threats possible and tempt threat actors to exploit them. Types of vulnerabilities in network security include but are not limited to SQL injections, server misconfigurations, cross-site scripting and transmitting sensitive data in a non-encrypted plain text format. When threat probability is multiplied by the potential loss that may result, cybersecurity experts refer to this as risk.

TYPES OF CYBER SECURITY THREATS

Just as there is a plethora of various germs and diseases that can attack the human body, there are numerous threats that can affect hardware, software and the information you store. Some of the major ones include the following:

- **Viruses**: similar to the way the common cold replicates itself repeatedly in one person's body and is then spread, a software virus is designed in such a way that can be easily transmitted from one computer or system to another. Often sent as email attachments, viruses corrupt and co-opt data, interfere with your security settings, generate spam and may even delete content.

- **Computer worms** are similar; they spread from one computer to the next by sending itself to all of the user's contacts and subsequently to all of the contacts' contacts.
- **Trojans**: these malicious pieces of software insert themselves into a legitimate program. Often, people voluntarily let trojans into their systems in the form of email messages from a person or an advertiser they trust. As soon as the accompanying attachment is open, your system becomes vulnerable to the malware within.
- **Bogus security software** that tricks users into believing that their system has been infected with a virus. The accompanying security software that the threat actor provides to fix the problem actually causes it.
- **Adware** that tracks your browsing habits and causes particular advertisements to pop up. Although this is common and often something you may even agree to, adware is sometimes foisted upon you without your consent. Similarly, spyware is an intrusion that may steal sensitive data such as passwords and credit card numbers from your internal systems.
- **Denial of service (DOS) attack**: this occurs when hackers deluge a website with traffic, making it impossible for users to access its content. A distributed denial of service (DDOS) attack is more forceful and aggressive since it is initiated from several servers simultaneously. As a result, a DDOS attack is harder to mount defenses against.
- **Phishing attacks** are social engineering infiltrations whose goal is to wrongfully obtain sensitive data such as passwords and credit card numbers. Via emails or links, the hacker causes malware to be downloaded and installed. Many phishing attacks appear to come from trusted companies and financial institutions and ask users to verify their identity, thus leaving them open to hacking.

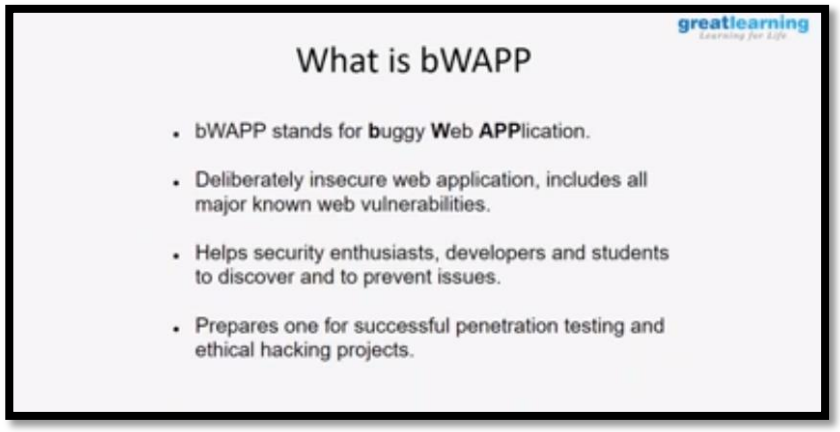
- **SQL injections** are network threats that involve using malicious code to infiltrate cyber vulnerabilities in data systems. As a result, data can be stolen, changed or destroyed. This type of attack is quickly becoming the most serious network security issue.
- **Man-in-the-middle attacks** involve a third party intercepting and exploiting communications between two entities that should remain private. Not only does eavesdropping occur but also information can be changed or misrepresented by the intruder, causing inaccuracy and even security breaches.
- **Rootkit tools** gain remote access to systems without permission and can lead to the installation of malware and the stealing of passwords and other data.

DAILY ASSESSMENT

Date:	**18/06/2020**	**Name:**	**Davis S. Patel**
Course:	**Ethical Hacking**	**USN:**	**4AL16EC045**
Topic:	**What is Ethical hacking? Ethical hacking on mobile platforms - Demonstration**	**Semester & Section:**	**8th - A**
GitHub Repository:	**Davis**		

AFTERNOON SESSION DETAILS

Images of Session



REPORT –

In the dawn of international conflicts, terrorist organizations funding cybercriminals to breach security systems, either to compromise national security features or to extort huge amounts by injecting malware and denying access. Resulting in the steady rise of cybercrime. Organizations face the challenge of updating hack-preventing tactics, installing several technologies to protect the system before falling victim to the hacker.

New worms, malware, viruses, and ransomware are multiplying every day and is creating a need for ethical hacking services to safeguard the networks of businesses, government agencies or defense.

Ethical hacking and ethical hacker are terms used to describe hacking performed by a company or individual to help identify potential threats on a computer or network. An ethical hacker attempts to bypass system security and search for any weak points that could be exploited by malicious hackers. This information is then used by the organization to improve the system security, to minimize or eliminate any potential attacks.

Web application provides an interface between the web server and the client to communicate. Web pages are generated at the server, and browsers present them at the client side. The data is passed between client and server in the form of HTML pages through HTTP protocol.

There are client-side vulnerabilities and server-side vulnerabilities which lead to a web application attack. Websites and web applications are—by their very nature—accessible remotely, which puts them at high risk of cyberattacks. Knowing how to detect and prevent web attacks is a critical skill for developers and information security professionals alike. In this course, find out how to test your sites and applications for weaknesses.

Cybersecurity expert Malcolm Shore examines the various parts of a web application and introduces the Open Web Application Security Project (OWASP), which provides documentation, tools, and forums for web developers and testers. He also provides an overview of popular testing tools, including Burp Suite and OWASP ZAP. Learn how to use these utilities to run basic and advanced tests, and protect sites against common attacks.

The web is also an excellent sales channel for a myriad of organizations, large or small: with over 1 billion Internet users (source: Computer Industry Almanac, 2006), US e-commerce spending accounted for $102.1 billion in 2006 (Source: comScore Networks, 2007). All this data must be somehow captured, stored, processed and transmitted to be used immediately or at a later date. Web applications, in the form of submit fields, inquiry, and login forms, shopping carts, and content management systems, are those website widgets that allow this to happen. They are, therefore, fundamental to businesses for leveraging their online presence thus creating long-lasting and profitable relationships with prospects and customers.