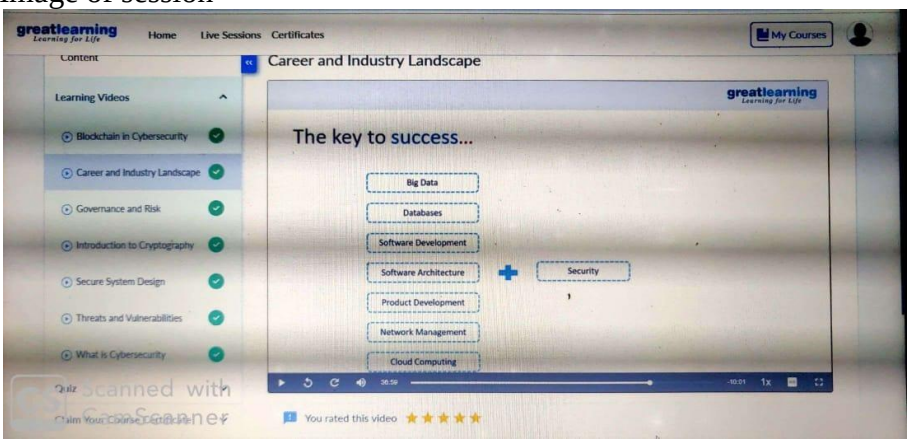
Daily Assessment Report

Date:	18/06/20	Name:	Gaganashree P
Course:	Cyber security	USN:	4AL15EC024
Topic:	1. Compliance, Governance and industry standards, Career and industry landscape & Program relevance	Semester & Section:	8TH & A
Github Repository:	Gaganashree-P		

FORENOON SESSION DETAILS

Image of session



Report – Report can be typed or hand written for up to two pages.

1. compliance

In general, compliance is defined as following rules and meeting requirements. In cybersecurity, compliance means creating a program that establishes risk-based controls to protect the integrity, confidentiality, and accessibility of information stored, processed, or transferred. However, cybersecurity compliance is not based in a stand-alone standard or regulation. Depending on the industry, different standards may overlap, which can create confusion and excess work for organizations using a checklist-based approach.

For example, the healthcare industry needs to meet Health Insurance Portability and Accountability Act (HIPAA) compliance requirements, but if a provider also accepts payments through a point-of-service (POS) device, then it also needs to meet Payment Card Industry Data Security Standard (PCI DSS) requirements. Moreover, as compliance requirements shift from control-based to risk-based, the landscape of cybersecurity compliance also shifts.

5 Steps to Creating a Cybersecurity Compliance Program

1. Create a Compliance Team

Even in small to mid-sized businesses, a compliance team is necessary. Cybersecurity does not exist in a vacuum. As organizations continue to move their business critical operations to the cloud, they need to create an interdepartmental workflow and communicate across business and IT departments.

2. Establish a Risk Analysis

As more standards and regulations focus on taking a risk-based approach to compliance, organizations of all sizes need to engage in the risk analysis process.

IDENTIFY

Identify all information assets and information systems, networks, and data that they access.

ASSESS RISK

Review the risk level of each data type. Determine where high risk information is stored, transmitted, and collected and rate the risk of those locations accordingly.

ANALYZE RISK

After assessing risk, you need to analyze risk. Traditionally, organizations use the following formula:

Risk = (Liklihood of Breach x Impact)/Cost

SET RISK TOLERANCE

After analyzing the risk, you need to determine whether to transfer, refuse, accept, or mitigate the risk.

3. Set Controls

Based on your risk tolerance, you need to determine how to mitigate or transfer risk. Controls can include:

Firewalls

Encryption

Password policies

Vendor risk management program

Employee training

Insurance

4. Create Policies

Policies document your compliance activities and controls. These policies serve as the foundation for any internal or external audits necessary.

5. Continuously Monitor and Respond

All compliance requirement focus on the way in which threats evolve. Cybercriminals continuously work to find new ways to obtain data. Rather than working to find new vulnerabilities, called Zero Day

Attacks, they prefer to rework existing strategies. For example, they may combine two different types of known ransomware programs to create a new one.

2. Governance and risk

Governance, Risk and Compliance (GRC)

With digital disruption rapidly pervading and positively impacting enterprises; Information Security Governance, Risk Management & Compliance (GRC) plays a pivotal role in sustainably managing risks. Prominence of Cloud Services and Internet of Things (IoT) has resulted in a distributed enterprise data with virtual network boundaries, throwing unique challenges to CIOs / CISOs. Regulators across the globe have re-emphasized the importance of data protection through a multitude of mandates, which enterprises must comply with.

A well-rounded GRC framework facilitates the formulation and sustained management of information security risks. Such a framework helps identify risks proactively & systematically, and enables the security governance function to achieve adequate and mature security with the desired levels of internal & external compliance.

3. Career and industry landscape

The landscape of security

At this point, we can begin to envision the landscape of security. There are actually two different illustrations that capture what I have described. The first is a layered picture: lower layers providing services to higher layers. Lower layers are more general: the packet transport layer of the Internet is very general–it just moves packets of data. On top of this a general application might be fashioned, such as the Web. In turn, on top of this a more specific service might be crafted, such as Facebook, and on top of this there might be specific “Facebook apps” that run in the context of Facebook. The Internet is a layer-cake of platforms, each supporting services on top of them.

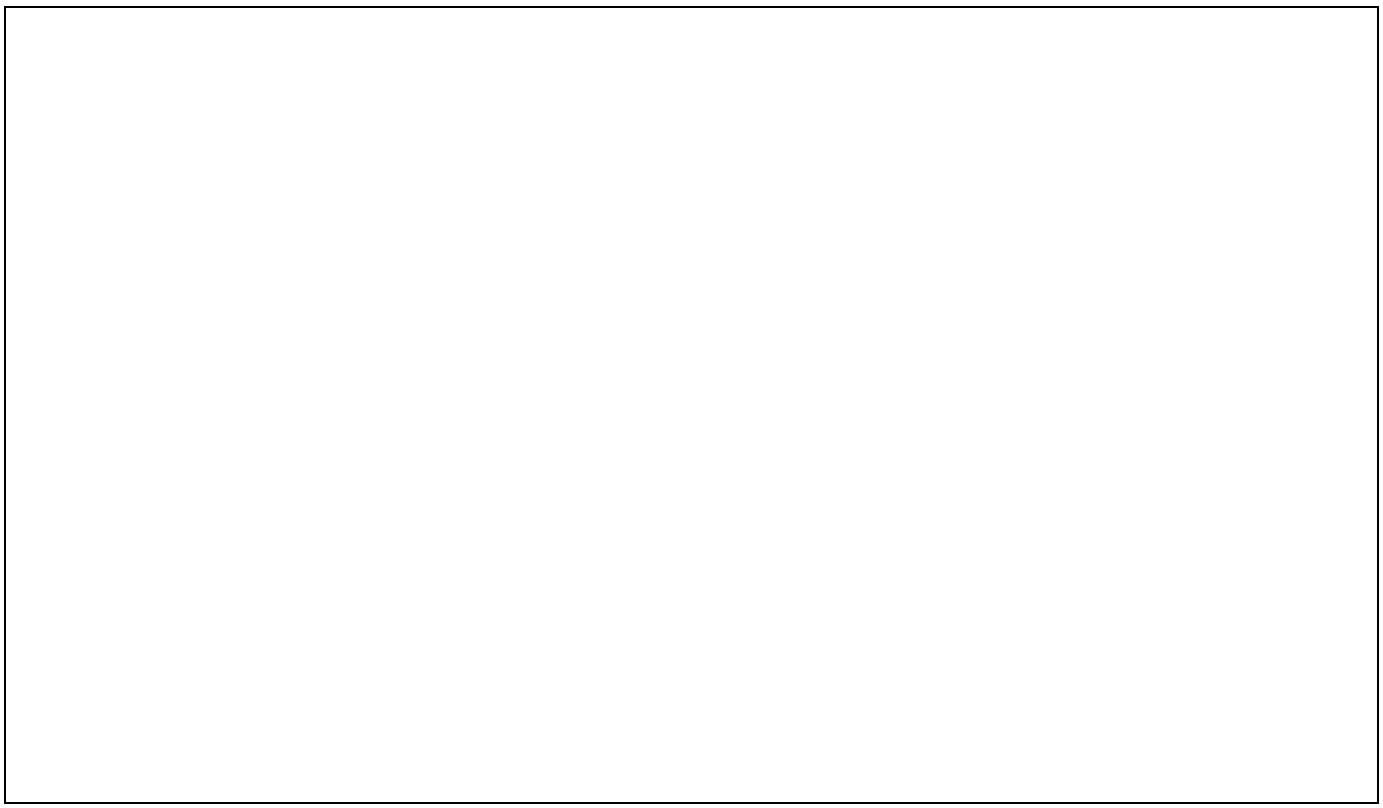
At each layer, the security analysis must include an analysis of the extent to which untrusted parties are either intentionally or unavoidably in the system, whether their actions can cause harm, and if so how to discipline those behaviors. In general, this responsibility cannot be “pushed down” into a lower layer, but it may be possible for

the lower layer to provide supporting services to make that task easier. The other illustration is a regional one, much like a map of the globe. We know that there are regions of the world we don't much trust. The same is true of the Internet; there are regions of the packet forwarding layer of the Internet (they are called Autonomous Systems, or ASes) that are not trustworthy, and regions can and do attack each other (in particular the routing protocols). And this regional structure is true at every layer: there are untrustworthy email senders, untrustworthy web sites, and so on. In the context of certain applications, if we can detect them we can try to eject them from the community of mutually trusting actors (this is what anti-abuse institutions such as Spamhaus try to do with spammers) but in general we have to accept that they are in the system, and must be tolerated, if not welcomed.

Mapping classic "security problems" into this landscape It is useful to take these illustrations of the security landscape and use them to try to position some of the well-known categories of "security problem".

Attacks on the network itself These include attacks on the routing protocols, attacks on critical supporting services such as the Domain Name Service (the DNS), and the like. Since the core function of the Internet is actually rather simple, there are only a few of these services; the interesting question is why they remain insecure. I return to this below. To the extent that this layer cannot detect and remedy these problems internally, the consequences of attacks at this layer will become visible to the layers above, which will have to take corrective action.

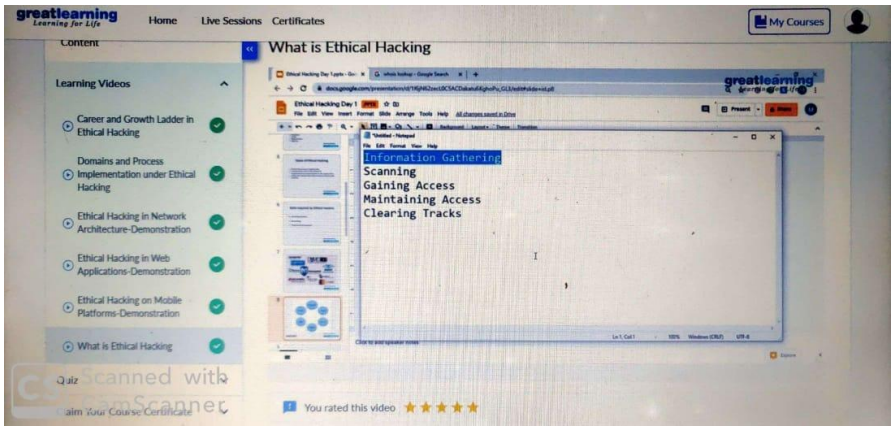
Attacks on attached hosts can occur as a result of communication with a malicious party (who uses the capabilities of one or another layer to deliver an attack) or as a result of an unsolicited incoming packet that somehow exploits a vulnerability to launch a successful attack. Over the years, these sorts of attacks have been "moving up the layers". In the past, there were some well-known vulnerabilities in the software that supported the packet transport layer–for example packets that would cause problems with the TCP layer. In most implementations, these have been fixed. Most operating systems today are reasonably secure against



Daily Assessment Report

Date:	**18/06/20**	**Name:**	**Gaganashree P**
Course:	**Ethical hacking**	**USN:**	**4AL15EC024**
Topic:	**1. Introduction to ethical hacking**	**Semester & Section:**	**8TH & A**
Github Repository:	**Gaganashree-P**		

Afternoon SESSION DETAILS
Image of session



Report – Report can be typed or hand written for up to two pages.

1.What is Ethical hacking?

Ethical Hacking is an authorized practice of bypassing system security to identify potential data breaches and threats in a network. The company that owns the system or network allows Cyber Security experts to perform such activities in order to test the system's defenses. Thus, unlike malicious hacking, this process is planned, approved, and more importantly, legal.

Ethical hackers aim to investigate the system or network for weak points that malicious hackers can exploit or destroy. They collect and analyze the information to figure out ways to strengthen the security of the system/network/applications. By doing so, they can improve the security footprint so that it can better withstand attacks or divert them.

Ethical Hackers check for key vulnerabilities include but are not limited to:

Injection attacks

Changes in security settings

Exposure of sensitive data

Breach in authentication protocols

Components used in the system or network that may be used as access points

Types of Hackers

The practice of ethical hacking is called "White Hat" hacking, and those who perform it are called White Hat hackers. In contrast to Ethical Hacking, "Black Hat" hacking describes practices involving security violations. The Black Hat hackers use illegal techniques to compromise the system or destroy information.

Unlike White Hat hackers, "Grey Hat" hackers don't ask for permission before getting into your system. But Grey Hats are also different from Black Hats because they don't perform hacking for any personal or third-party benefit. These hackers do not have any malicious intention and hack systems for fun or various other reasons, usually informing the owner about any threats they find. Grey Hat and Black Hat hacking are both illegal as they both constitute an unauthorized system breach, even though the intentions of both types of hackers differ.

White Hat vs Black Hat Hacker

The best way to differentiate between White Hat and Black Hat hackers is by taking a look at their motives. Black Hat hackers are motivated by malicious intent, manifested by personal gains, profit, or harassment; whereas White Hat hackers seek out and remedy vulnerabilities, so as to prevent Black Hats from taking advantage.

The other ways to draw a distinction between White Hat and Black Hat hackers

include:

Techniques used: White Hat hackers duplicate the techniques and methods followed by malicious hackers in order to find out the system discrepancies, replicating all the latter's steps to find out how a system attack occurred or may occur. If they find a weak point in the system or network, they report it immediately and fix the flaw.

Legality: Even though White Hat hacking follows the same techniques and methods as Black Hat hacking, only one is legally acceptable. Black Hat hackers break the law by penetrating systems without consent.

Ownership: White Hat hackers are employed by organizations to penetrate their systems and detect security issues. Black hat hackers neither own the system nor work for someone who owns it.

Roles and Responsibilities of an Ethical Hacker

Ethical Hackers must follow certain guidelines in order to perform hacking legally. A good hacker knows his or her responsibility and adheres to all of the ethical guidelines. Here are the most important rules of Ethical Hacking:

* An ethical hacker must seek authorization from the organization that owns the system. Hackers should obtain complete approval before performing any security assessment on the system or network.

* Determine the scope of their assessment and make known their plan to the organization.

* Report any security breaches and vulnerabilities found in the system or network.

* Keep their discoveries confidential. As their purpose is to secure the system or network, ethical hackers should agree to and respect their non-disclosure agreement.

* Erase all traces of the hack after checking the system for any vulnerability. It prevents malicious hackers from entering the system through the identified loopholes.

Benefits of Ethical Hacking

Learning ethical hacking involves studying the mindset and techniques of black hat hackers and testers to learn how to identify and correct vulnerabilities within networks. Studying ethical hacking can be applied by security pros across industries and in a multitude of sectors. This sphere includes network defender, risk management, and quality assurance tester.

However, the most obvious benefit of learning ethical hacking is its potential to inform and improve and defend corporate networks. The primary threat to any organization's security is a hacker: learning, understanding, and implementing how hackers operate can help network defenders prioritize potential risks and learn how to remediate them best. Additionally, getting an ethical hacking training or certifications can benefit those who are seeking a new role in the security realm

or those wanting to demonstrate skills and quality to their organization.

Skills Required to Become an Ethical Hacker

An ethical hacker should have in-depth knowledge about all the systems, networks, program codes, security measures, etc. to perform hacking efficiently. Some of these skills include:

Knowledge of programming - It is required for security professionals working in the field of application security and Software Development Life Cycle (SDLC).

Scripting knowledge - This is required for professionals dealing with network-based attacks and host-based attacks.

Networking skills - This skill is important because threats mostly originate from networks. You should know about all of the devices present in the network, how they are connected, and how to identify if they are compromised.

Understanding of databases - Attacks are mostly targeted at databases. Knowledge of database management systems such as SQL will help you to effectively inspect operations carried out in databases.

Knowledge of multiple platforms like Windows, Linux, Unix, etc.

The ability to work with different hacking tools available in the market.

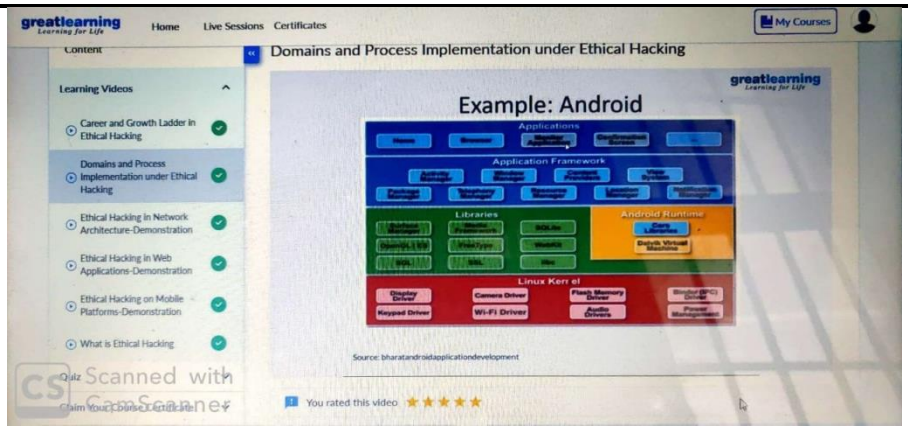
Knowledge of search engines and servers.

Tools for hacking

2.ethical hacking in web application -demonstration

Hacking Web Applications

Web applications provide an interface between end users and web servers through a set of web pages generated at the server end or that contain script code to be executed dynamically within the client Web browser.



Hacking Web Applications Exercises

Ethical Hacking Exercises / Hacking Web Applications contains the following Exercises:

* Hacking Web Applications

* Website Vulnerability Scanning Using Acunetix WVS

Web Application and its types of Attacks

Introduction

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.

Attacks:

Parameter Tampering:

This involves modifying parameters exchanged between client and server, which may lead to XSS attack and SQL injection attack. Usually, HTML data goes as a name-value pair; if the attacker is able to modify the values of the parameter during transfer, it may lead to many other attacks.

Unvalidated inputs:

Web applications accept user inputs, queries are constructed based on dynamic user input. If these inputs are not properly sanitised they will open a way for the attacker to launch attacks like XSS, SQL injection attack, Directory traversal attack, etc., identity theft, data theft are dangerous outcomes of this attack.

Directory traversal Attack:

This is a type of vulnerability where an attacker is able to access beyond the web root directory, into the restricted directories on the web server. Then an attacker will be able to access system files, run OS commands, access configuration information, etc.