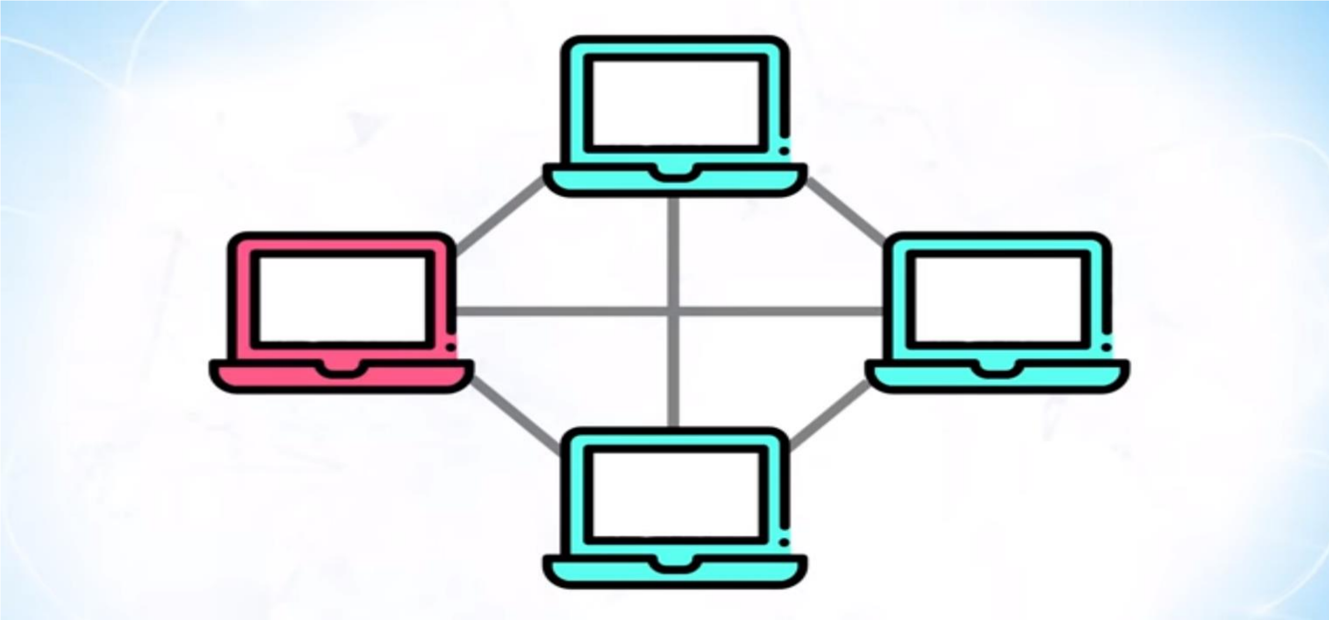
DAILY ASSESSMENT FORMAT

Date:	18th June 2020	**Name:**	Soundarya NA
Course:	Cyber security	**USN:**	4AL16EC077
Topic:	Cyber security	**Semester & Section:**	8th - B

FORENOON SESSION DETAILS

Image of session



Report:

Ciphers and encryption:

In cryptology, the discipline concerned with the study of cryptographic algorithms, a cipher is an algorithm for encrypting and decrypting data. Symmetric key encryption, also called secret key encryption, depends on the use of ciphers, which operate symmetrically. With symmetric algorithms, the same cipher and encryption key are applied to data in the same way, whether the objective is to convert plaintext to ciphertext or ciphertext to plaintext. A cipher transforms data by processing the original, plaintext characters (or other data) into ciphertext, which should appear to be random data.

Traditionally, ciphers used two main types of transformation: transposition ciphers, which keep all the original bits of data in a byte but mix their order, and substitution ciphers, which replace specific data sequences with other specific data sequences. For example, one type of substitution would be to transform all bits with a value of 1 to a value of 0, and vice versa. The data output by either method is called the ciphertext.

Modern ciphers enable private communication in many different networking protocols, including the Transport Layer Security (TLS) protocol and others that offer encryption of network traffic. Many communication technologies, including phones, digital television and ATMs, rely on ciphers to maintain security and privacy.

A cipher uses a system of fixed rules an algorithm to transform plaintext, a legible message, into ciphertext, an apparently random string of characters. Ciphers can be designed to encrypt or decrypt bits in a stream (stream ciphers), or they can process ciphertext in uniform blocks of a specified number of bits (block ciphers).

Modern cipher implementations depend on the cipher algorithm and a secret key, which is used by the cipher algorithm to modify data as it is encrypted. Ciphers that use longer keys, measured in bits, can be more secure from brute-force attacks, because the longer the key length, the more brute-force attempts are necessary to expose the plaintext. While cipher strength is not always dependent on the length of the key, experts recommend modern ciphers be configured to use keys of at least 128 bits to 1,024 bits or more, depending on the algorithm and the use case.

A key is an essential part of a cipher algorithm -- so much so that, in real-world ciphering, the key is kept secret, not the algorithm. Strong ciphers are designed so that, even if someone knows the algorithm, it should be virtually impossible to decipher a ciphertext without knowing the appropriate key. Consequently, before a cipher can work, both the sender and receiver must have a key or set of keys.

5 common encryption algorithms:

1. **Triple DES:** Triple DES was designed to replace the original Data Encryption Standard (DES) algorithm, which hackers eventually learned to defeat with relative ease. At one time, Triple DES was the recommended standard and the most widely used symmetric algorithm in the industry.

   Triple DES uses three individual keys with 56 bits each. The total key length adds up to 168 bits, but experts would argue that 112-bits in key strength is more like it.

   Despite slowly being phased out, Triple DES still manages to make a dependable hardware encryption solution for financial services and other industries.

2. **RSA:** RSA is a public-key encryption algorithm and the standard for encrypting data sent over the internet. It also happens to be one of the methods used in our PGP and GPG programs. Unlike Triple DES, RSA is considered an asymmetric algorithm due to its use of a pair of keys. You've got your public key, which is what we use to encrypt our message, and a private key to decrypt it. The result of RSA encryption is a huge batch of mumbo jumbo that takes attackers quite a bit of time and processing power to break.

3. **Blowfish:** Blowfish is yet another algorithm designed to replace DES. This symmetric cipher splits messages into blocks of 64 bits and encrypts them individually.

Blowfish is known for both its tremendous speed and overall effectiveness as many claim that it has never been defeated. Meanwhile, vendors have taken full advantage of its free availability in the public domain.

Blowfish can be found in software categories ranging from e-commerce platforms for securing payments to password management tools, where it used to protect passwords. It's definitely one of the more flexible encryption methods available.

4. **Twofish:** Computer security expert Bruce Schneier is the mastermind behind Blowfish and its successor Twofish. Keys used in this algorithm may be up to 256 bits in length and as a symmetric technique, only one key is needed.

   Twofish is regarded as one of the fastest of its kind, and ideal for use in both hardware and software environments. Like Blowfish, Twofish is freely available to anyone who wants to use it. As a result, you'll find it bundled in encryption programs such as PhotoEncrypt, GPG, and the popular open source software TrueCrypt.

5. **AES:** The Advanced Encryption Standard (AES) is the algorithm trusted as the standard by the U.S. Government and numerous organizations.
   Although it is extremely efficient in 128-bit form, AES also uses keys of 192 and 256 bits for heavy duty encryption purposes.

   AES is largely considered impervious to all attacks, with the exception of brute force, which attempts to decipher messages using all possible combinations in the 128, 192, or 256-bit cipher. Still, security experts believe that AES will eventually be hailed the de facto standard for encrypting data in the private sector.

Block chain and cyber security:

The technology behind the infamous cryptocurrency Bitcoin, blockchain, is becoming increasingly popular as cybersecurity experts look for more ways to fight cybercrime and data breach. Consumers are also becoming more and more proactive in terms of their cybersecurity, opening to alternatives that can promise better connectivity at heightened security.

Dubbed as the new and safer internet, blockchain makes it possible for data to be distributed without duplication, different from the current structure the internet has today. In this article, we’re going to have a look at how blockchain contributes to cybersecurity.

Blockchain technology is a decentralised distributed ledger system where you can put any digital asset into the blockchain, regardless of industry. It uses a time-stamped series of immutable records of information managed by a cluster of computers. Different transactions are tracked through these records, separated by blocks, and joined by cryptographic chains. Data is not owned by a single computer or entity, but by multiple users within the system.

Once confirmed, data that has been encoded cannot be altered. They become permanent blocks added to a chain of other validated blocks. Initially devised for cryptocurrencies, the digital community is now seeing the enormous potential of blockchain technology in cybersecurity, as it can be used to prevent cyber-attacks, data breaches, identity thefts, or malicious transactions, keeping data private and secure.

Blockchain presents itself as a backbone to different technologies, providing solutions that are beneficial across different industries. It’s main characteristics are:

- Blockchain has a democratised network and has no central authority. It is public domain, so there can be no one or no group that can come in to manipulate information within the blockchain system for any malicious intent
- The blockchain is a decentralised system NOT owned by one entity. Data in the blockchain system can be cryptographically stored
- Whatever gets stored in a blockchain is immutable, preventing anyone from tampering or manipulating information. With blockchain, it is possible, for example, to hold a completely

transparent election with immediate results. People can vote at their homes, and the results tallied right away

- The blockchain is transparent – Whatever gets built and stored in the blockchain is openly accessible. The data stored inside can also be tracked, holding a higher standard of accountability for those using the system

How can blockchain technology contribute to cybersecurity?

Protected Edge Computing with Authentication:

As more and more real-time, on-demand data need to be accessed and distributed, there's also a need for edge computing and fog computing devices and storage. This allows data to be processed and stored closer to the source and consumers. Cloud computing is still being used, of course, primarily to archive data previously processed through edge computing devices. Blockchain is providing a solution to secure IoT and industrial IoT by more rigid authentication, improved data attribution and flow, and updated record management system.

Advanced Confidentiality and Data Integrity:

Because it was initially intended to be publicly-accessed, blockchain was made without access controls or restrictions. Today, there are private blockchain systems that various industries are using to ensure data confidentiality and secure access control. The complete encryption of the blockchain makes sure that data is not accessible to external parties, whether in part or whole, particularly while data is being transmitted.

Secured Private Messaging:

Companies hope to communicate through more secure platforms using the blockchain technology that can be impenetrable to malicious attacks. Whether in personal, corporate or highly-classified communication, consumers can be secured with the confidentiality of such conversations without fear of cyberattacks. It can handle PKI better than encrypted apps; that is why several blockchain private messaging apps are being developed for public consumption soon.

Improved PKI:

People are more cautious to keep their computer and online credentials safe and secure. And blockchain technology can help in that regard. Public Key Infrastructure (PKI) rely on third-party certificate authorities to keep messaging apps, emails, websites secure. These certificate authorities that issue, revoke or store key pairs are usually a target for hackers using bogus identities trying to access communication that is encrypted. When these keys are encoded on a blockchain, it minimizes false key generation or identity theft as identities of legitimate account holders are already verified on the app, and any intrusion, deception or identity theft can be identified right away.

Intact Domain Name System (DNS):

A blockchain approach to storing Domain Name Systems (DNS) heightens security comprehensively as it removes that one, single, comprisable target. It thwarts the malicious activities of hackers who can bring down DNS service providers like Twitter, Paypal and the like.

Diminished DDoS attacks:

In a distributed denial-of-service (DDoS) attack, a target, usually, a server, is attacked by multiple compromised computer systems to deny it of services leading to slowdowns, and eventual overloading or crashing of the system. If you integrate blockchain into the security system, the target computer, server or network will now be part of a decentralised system of machines which can protect against such attacks.

We can develop and adopt multiple measures for security, and yet threats develop and adapt accordingly. However, with blockchain, we have a vast scope of ensuring data is safe.

Internet of Things (IoT):

Smart systems continue to be developed towards the future implementation of smart cities and societies in the future, and the Internet of Things (IoT) is in the middle of all this action. From your coffee maker to AI-powered robots in aid of humans, IoT will have its mark everywhere. As of date, cybercriminals continue to find ways to attack these IoT smart devices. Blockchain technology's immutability will serve well if incorporated into the IoT's defense systems.

Blockchain technology, with its decentralized architecture and distributed ledger, will provide both control and security for remote IoT devices. Smart contracts, which can provide validation for transactions in a blockchain environment, may be used to manage IoT activities and keep devices secure from hackers.

Relevance:

Cybersecurity risk is increasing, driven by global connectivity and usage of cloud services, like Amazon Web Services, to store sensitive data and personal information. Widespread poor configuration of cloud services paired with increasingly sophisticated cyber criminals means the risk that your organization suffers from a successful cyber-attack or data breach is on the rise.

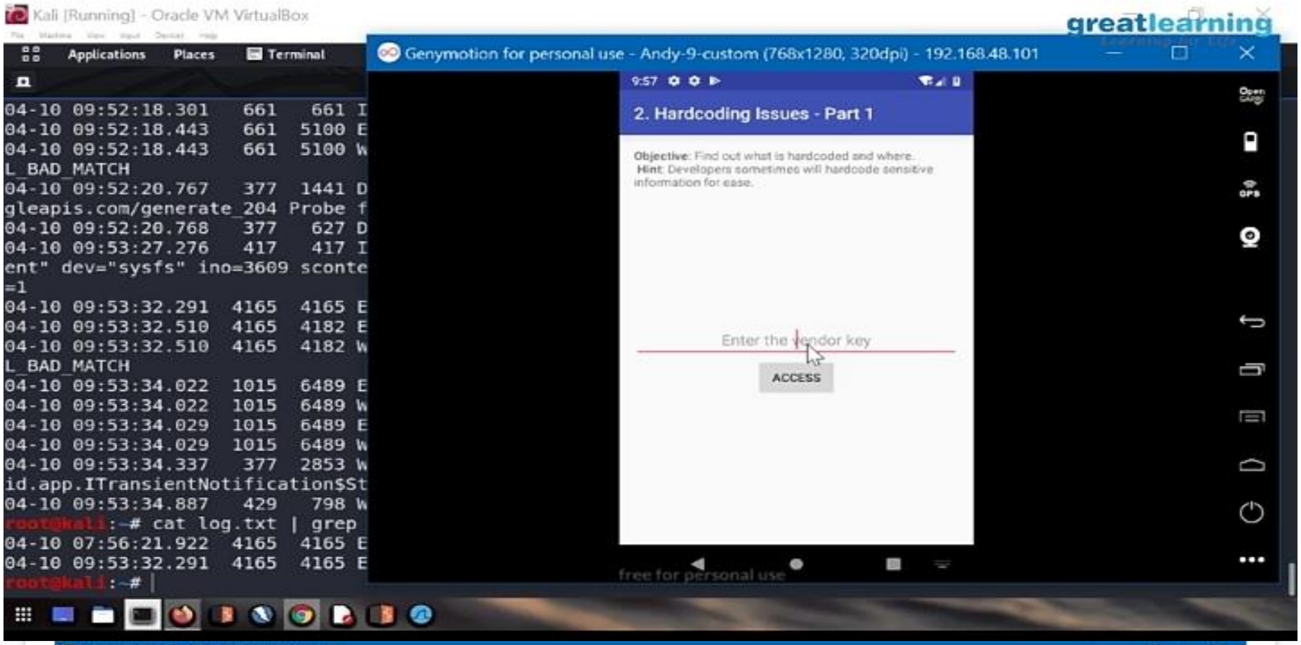
Gone are the days of simple firewalls and antivirus software being your sole security measures. Business leaders can no longer leave information security to cybersecurity professionals.

Cyber threats can come from any level of your organization. You must educate your staff about simple social engineering scams like phishing and more sophisticated cybersecurity attacks like ransomware (think WannaCry) or other malware designed to steal intellectual property or personal data.

GDPR and other laws mean that cybersecurity is no longer something businesses of any size can ignore. Security incidents regularly affect businesses of all sizes and often make the front page causing irreversible reputational damage to the companies involved.

AFTERNOON SESSION			
Date:	18th June 2020	**Name:**	Soundarya NA
Course:	Great learning	**USN:**	4AL16EC077
Topic:	Ethical hacking	**Semester & Section:**	8th - B

Image:


Kali [Running] - Oracle VM VirtualBox
Applications
Places
Terminal
greatlearning
Genymotion for personal use - Andy-9-custom (768x1280, 320dpi) - 192.168.48.101
9:57
free for personal use

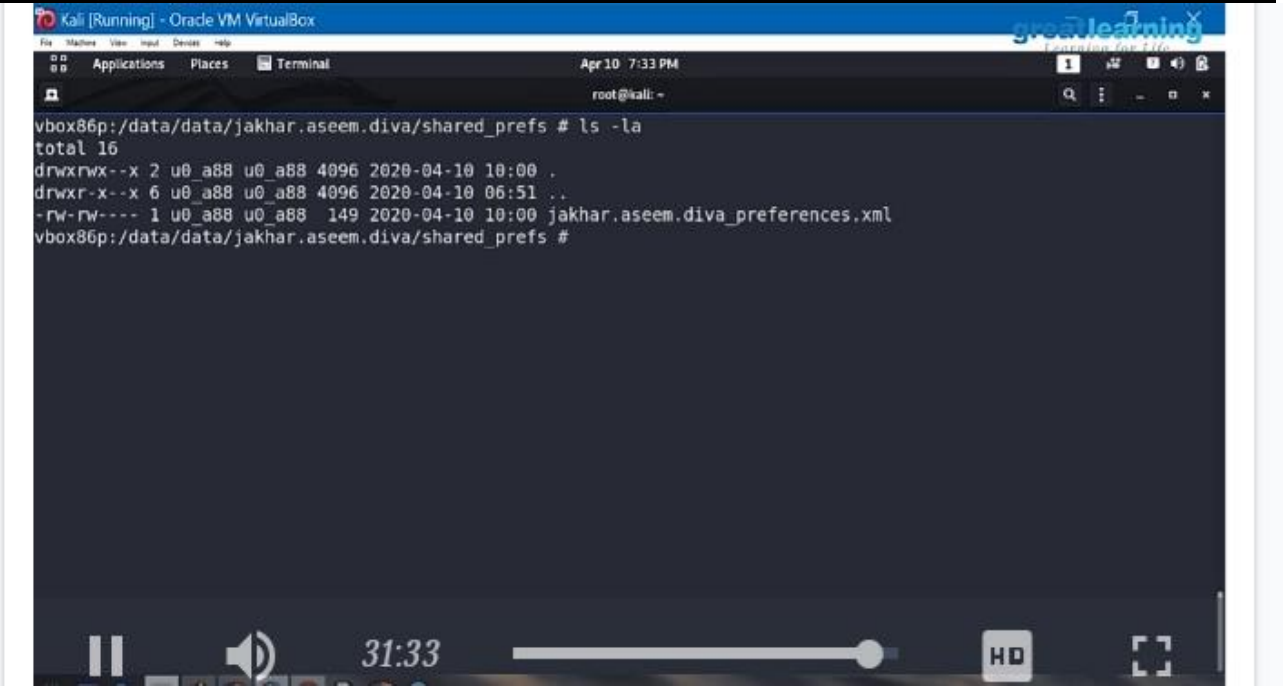
```
04-10 09:52:18.301   661   661 I
04-10 09:52:18.443   661  5100 E
04-10 09:52:18.443   661  5100 W
L_BAD_MATCH
04-10 09:52:20.767   377  1441 D
gleapis.com/generate_204 Probe f
04-10 09:52:20.768   377   627 D
04-10 09:53:27.276   417   417 I
ent" dev="sysfs" ino=3609 sconte
=1
04-10 09:53:32.291  4165  4165 E
04-10 09:53:32.510  4165  4182 E
04-10 09:53:32.510  4165  4182 W
L_BAD_MATCH
04-10 09:53:34.022  1015  6489 E
04-10 09:53:34.022  1015  6489 W
04-10 09:53:34.029  1015  6489 E
04-10 09:53:34.029  1015  6489 W
04-10 09:53:34.337   377  2853 W
id.app.ITransientNotification$St
04-10 09:53:34.887   429   798 W
root@kali:~# cat log.txt | grep
04-10 07:56:21.922  4165  4165 E
04-10 09:53:32.291  4165  4165 E
root@kali:~# |
```

2. Hardcoding Issues - Part 1

Objective: Find out what is hardcoded and where.
Hint: Developers sometimes will hardcode sensitive information for ease.

Enter the vendor key

ACCESS



```
vbox86p:/data/data/jakhar.aseem.diva/shared_prefs # ls -la
total 16
drwxrwx--x 2 u0_a88 u0_a88 4096 2020-04-10 10:00 .
drwxr-x--x 6 u0_a88 u0_a88 4096 2020-04-10 06:51 ..
-rw-rw---- 1 u0_a88 u0_a88  149 2020-04-10 10:00 jakhar.aseem.diva_preferences.xml
vbox86p:/data/data/jakhar.aseem.diva/shared_prefs #
```

Report:

What is Ethical Hacking?

Ethical Hacking sometimes called as Penetration Testing is an act of intruding/penetrating into system or networks to find out threats, vulnerabilities in those systems which a malicious attacker may find and exploit causing loss of data, financial loss or other major damages. The purpose of ethical hacking is to improve the security of the network or systems by fixing the vulnerabilities found during testing. Ethical hackers may use the same methods and tools used by the malicious hackers but with the permission of the authorized person for the purpose of improving the security and defending the systems from attacks by malicious users.

Ethical hackers are expected to report all the vulnerabilities and weakness found during the process to the management.

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.

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.