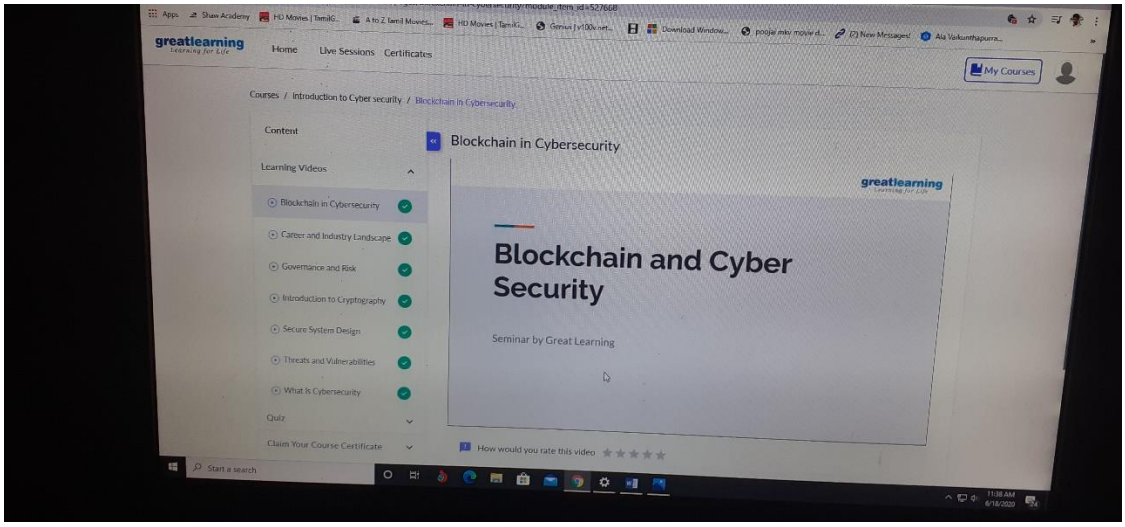
DAILY ASSESSMENT

Date:	**18-6-2020**	**Name:**	**Kavyashree m**
Course:	**Cyber security**	**USN:**	**4al15ec036**
Topic:	**Ciphers and encryption, Block chain and cyber security**	**Semester & Section:**	**8th A**
Github Repository:	**kavya**		

FORENOON SESSION DETAILS



Ciphers and encryption

Cipher is a global cybersecurity company that delivers a wide range of services. Get peace of mind with protection from cyber threats and hacking. In cryptography, a cipher (or cypher) is an algorithm for performing encryption or decryption—a series of well-defined steps that can be followed as a procedure. An alternative, less common term is decipherment. To encipher or encode is to convert information into cipher or code. In common parlance, "cipher" is synonymous with "code", as they are both a set of steps that

encrypt a message; however, the concepts are distinct in cryptography, especially classical cryptography.

Encryption is performed by keys, but it's important to square how keys and algorithms/ciphers fit together.

The algorithm or cipher used is just that, it's a sequence of steps that must be used to encrypt the plaintext.

Depending on the cryptosystem, either the values within that algorithm, or the value the algorithm arrives at itself, are the keys.

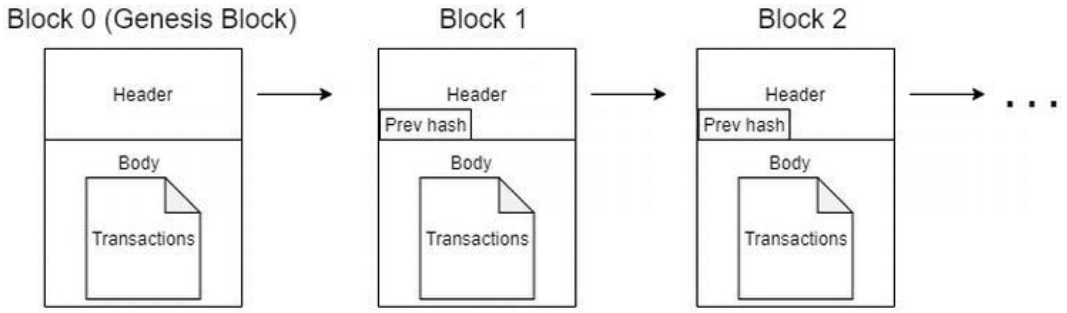
We'll clarify that point in a minute, just think of it this way: the algorithms are the general principles/rules used by a given cryptosystem, the keys are what actually performs the function.

Block chain and cyber security

Block chain is gaining traction today, but critics who question the scalability, security, and sustainability of the technology remain. Although some of block chains underlying capabilities provide data confidentiality, integrity and availability, just like other systems, cyber security controls and standards need to be adopted for organizations using block chains in order to protect their organizations from external attacks.

Block chain presents itself as a distributed ledger, referring this concept to the way a database is shared between several participants on a peer-to-peer network, without a central authority overseeing the process. In the case of block chain, this ledger is arranged, as its name suggests, in an ordered chain of blocks, each of which agglutinates transactions in order. A block, therefore, is basically a structure composed of a header and a body containing transactions in order. Blocks are timestamped and signed by its creator. The way these blocks constitute a chain is through a pointer to the previous block; the

header of each block contains a cryptographic hash of the previous block so that a block is linked to the previous one (while ensuring the immutability of that previous block). The very first block from which a block chain is constituted is known as the “genesis block”.



Block chain for backup and recovery

One of the most innovative applications of block chain technologies is to use it by secure storage and recovery systems. A Backup & recovery system usually has the following features:

- Continuous/Automatic data backup: It ensures that the changes you make to your files are simultaneously copied to the storage location. This lets you recover even the most recent changes in case of data loss, thus lowering your recovery point objective.
- Incremental backup: This is a type of backup where only the changes are copied, not the full file. This reduces the time taken for copying data and does not slow down your work.
- Instant recovery: This feature allows a backup snapshot to run temporarily on secondary storage to reduce the downtime of an application.
- Data deduplication: It eliminates duplicate data record blocks while data is transferred to the backup storage location. This reduces the network load and the storage space you require.

- Error-free copy: Data backup software features also ensure that the data copied from a source and stored at the backup server are the same and do not mismatch nor contain errors.
- Historically, backup and recovery procedures were applied mainly to general-purpose devices in the enterprise environment. The number of incidents grows daily, and the consequences are increasingly alarming as, for example, security holes in IP cameras [6], DDOS attacks generated from the Mirai botnet [7, 8] known as Dyn Attack or event take control of a vehicle [9]. Due to these problems, Backup & Recovery systems are being extended to cover these devices too.

Distributed file system (DFS)

When we find use cases such as the previous ones that require a distributed storage it is necessary to resolve where to store the files and who can access them. Block chain technology does not offer storage solutions and it is not a recommended practice to store files in the block chain. A possible solution is the use of distributed storage systems, like the decentralized P2P file storage systems. When using this kind of storage, files are divided into pieces that are replicated in different peers. A peer requiring access to an archive collects pieces of this archive, which is partially located in several peers at a time. The performance is similar to that of the P2P Bit Torrent network and files are indexed by their hash or fingerprint.

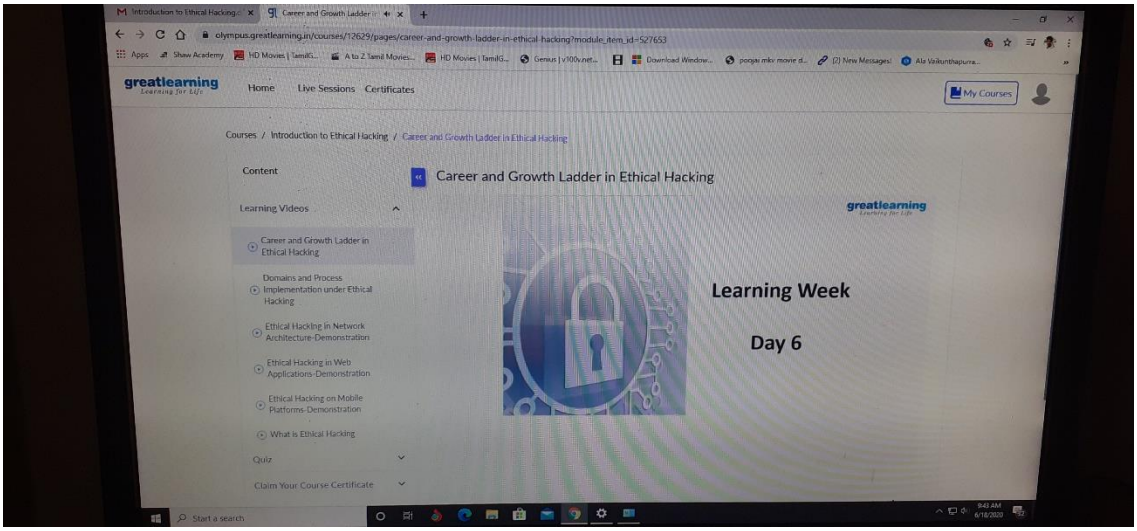
Block chain and content delivery networks (CDN)

Another interesting use case, maybe not so known as the previous one, is the application of block chain strategies to content delivery networks. These networks are widely used nowadays, so we have considered that they are a good example of how we can use block chain to add value to existent processes or technologies.

AFTERNOON SESSION DETAILS

Date:	**18-6-2020**	**Name:**	**Kavyashree m**
Course:	**Ethical hacking**	**USN:**	**4al15ec036**
Topic:	**Ethical hacking, Why is it a necessary Skill, Domains and process implementation under ethical hacking, Ethical hacking in web applications ,Demonstration**	**Semester & Section:**	**8th A**
Github Repository:	**kavya**		

Image of session



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.

Why is it a necessary skill

While you're building your cyber security résumé, work on developing hard IT skills like the ones listed below. These are often in high demand by employers. Since technology is always subject to change, we also recommend you consult your colleagues, mentors and/or professors for the most up-to-date advice.

Operating Systems & Database Management

- Windows, UNIX and Linux operating systems
- MySQL/SQLite environments

Programming & Coding

- C, C++, C# and Java
- Python, Ruby, PHP, Perl and/or shell
- Assembly language & disassemblers
- Regular Expression (regex) skills
- Linux/MAC Bash shell scripting

Networks

- System/network configuration
- TCP/IP, computer networking, routing and switching
- Network protocols and packet analysis tools
- Firewall and intrusion detection/prevention protocols
- Packet Shaper, Load Balancer and Proxy Server knowledge
- VPNs

Specializations

Thanks to the nature of their job and industry, security experts usually end up specializing in a specific area of interest. For example:

- Cisco networks
- Cloud computing
- Microsoft technologies
- Wireless
- Database modeling
- Open source applications
- Cryptography

And so on. To gain extra experience in these areas, you can volunteer for tasks at work, collaborate with a mentor and/or invest in self-directed learning and guided training.

Domains and process implementation under ethical hacking

An ethical hacker should have a wide range of computer skills. They often specialize, becoming subject matter experts (SME) on a particular area within the ethical hacking domain.

All ethical hackers should have:

- Expertise in scripting languages.
- Proficiency in operating systems.
- A thorough knowledge of networking.
- A solid foundation in the principles of information security.

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.

Ethical hacking in web application

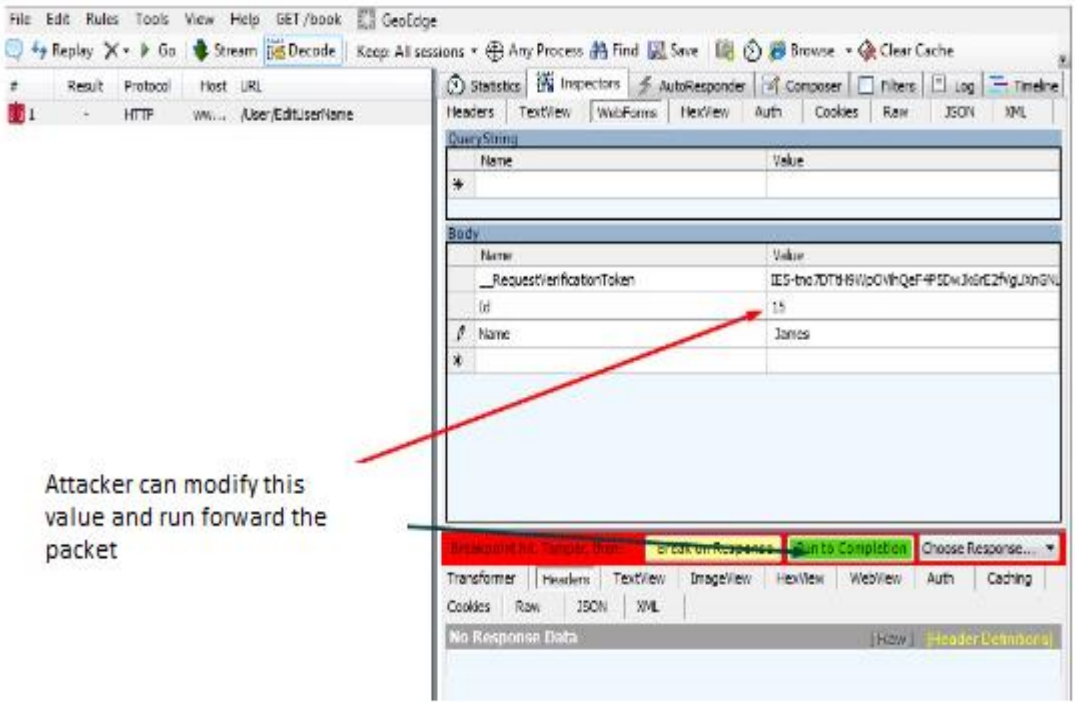
Web application provides an interface between the web server and the client to communicate. Web pages are generated at the server, and browsers present them at the client side. The data is passed between client and server in the form of HTML pages through HTTP protocol.

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.

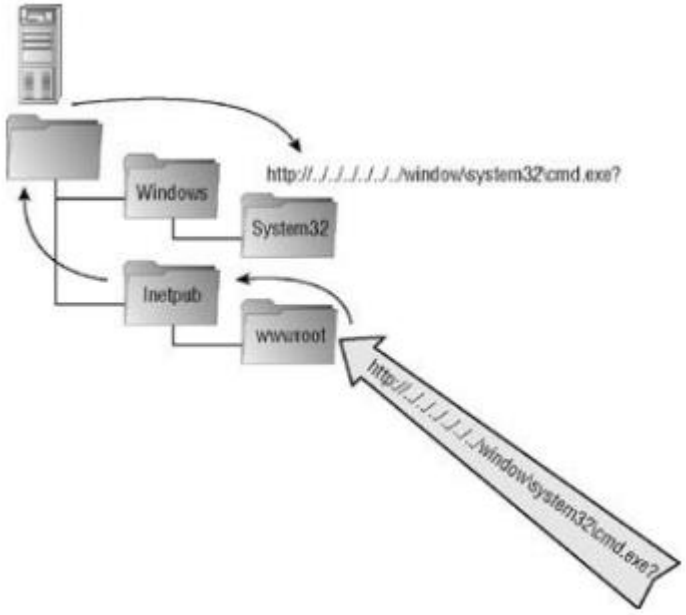


Invalidated inputs:

Web applications accept user inputs; queries are constructed based on dynamic user input. If these inputs are not properly sanitized 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.



Demonstration of ethical hacking

Certified Ethical Hacker (CEH) is a qualification obtained by demonstrating knowledge of assessing the security of computer systems by looking for weaknesses and vulnerabilities in target systems, using the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system. This knowledge is assessed by answering multiple choice questions regarding various ethical hacking techniques and tools. The code for the C|EH exam is 312-50. This certification has now

been made a baseline with a progression to the C|EH (Practical), launched in March 2018, a test of penetration testing skills in a lab environment where the candidate must demonstrate the ability to apply techniques and use penetration testing tools to compromise various simulated systems within a virtual environment.

Ethical hackers are employed by organizations to penetrate networks and computer systems with the purpose of finding and fixing security vulnerabilities. The EC-Council offers another certification, known as Certified Network Defense Architect (CNDA). This certification is designed for United States Government agencies and is available only to members of selected agencies including some private government contractors, primarily in compliance to DOD Directive 8570.01-M. It is also ANSI accredited and is recognized as a GCHQ Certified Training (GCT).

Examination

Certification is achieved by taking the C|EH examination after having either attended training at an Accredited Training Center (ATC), or completed through EC-Council's learning portal, I Class. If a candidate opts to self-study, an application must be filled out and proof submitted of two years of relevant information security work experience. Those without the required two years of information security related work experience can request consideration of educational background. The current version of the C|EH is V10 which uses the EC-Council's exam code 312-50, as the earlier versions did. The cost of CEH V10 is $1199. Although the new version V10 has recently been launched, this exam has 125 multiple-choice questions, with a 4-hour time limit, The EC-Council and various ATCs administer the C|EH examination. Members holding the C|EH/CNDA designation must seek re-certification under this program every three years, for a minimum of 120 credits