DAILY ONLINE ACTIVITIES SUMMARY

Date:	**02-06-2020**	**Name:**	**Manikya K**
Sem & Sec	**8th,A**	**USN:**	**4AL16CS050**
Online Test Summary			
Subject	**Not Conducted**		
Max. Marks	**-**	**Score**	**-**
Certification Course Summary			
Course	**1) Introduction to ethical hacking** **2) Introduction to cyber security**		
Certificate Provider	**Great learner academy**	**Duration**	**Ethical hacking - 6 Hrs** **Cyber Security - 7 Hrs**
Coding Challenges			
Problem Statement: c++ prog to find sum of digits until the number is a single digits			
Status: Solved			
Uploaded the report in Github	**Yes**		
If yes Repository name	**manikya-20**		
Uploaded the report in slack	**Yes**		

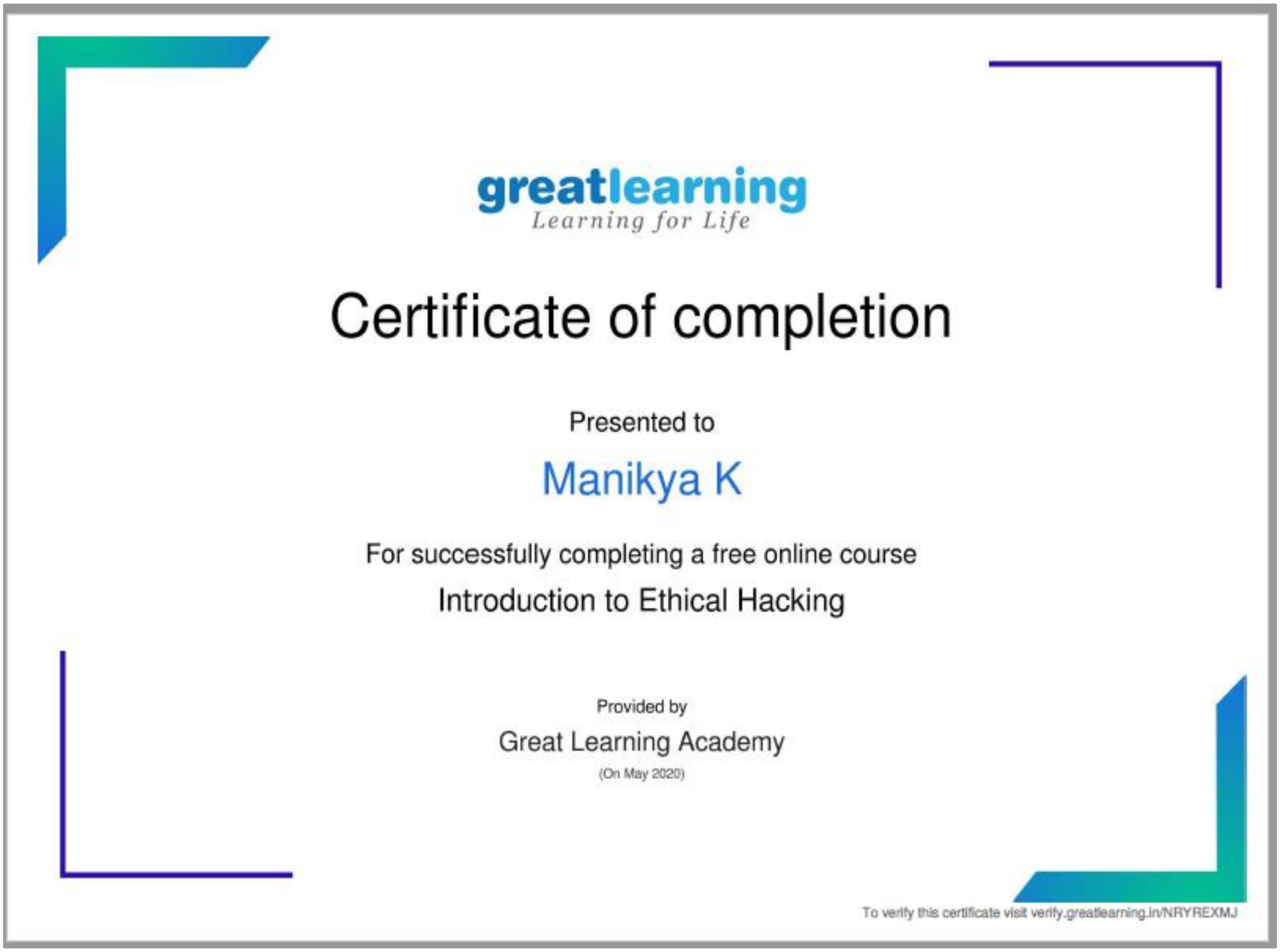
Online Test Details: (Attach the snapshot and briefly write the report for the same)

Certification Course Details: (Attach the snapshot and briefly write the report for the same)

Coding Challenges Details: (Attach the snapshot and briefly write the report for the sam

1) Certification Course Details:

A) Introdution to ethical hacking:



greatlearning

Learning for Life

Certificate of completion

Presented to

Manikya K

For successfully completing a free online course

Introduction to Ethical Hacking

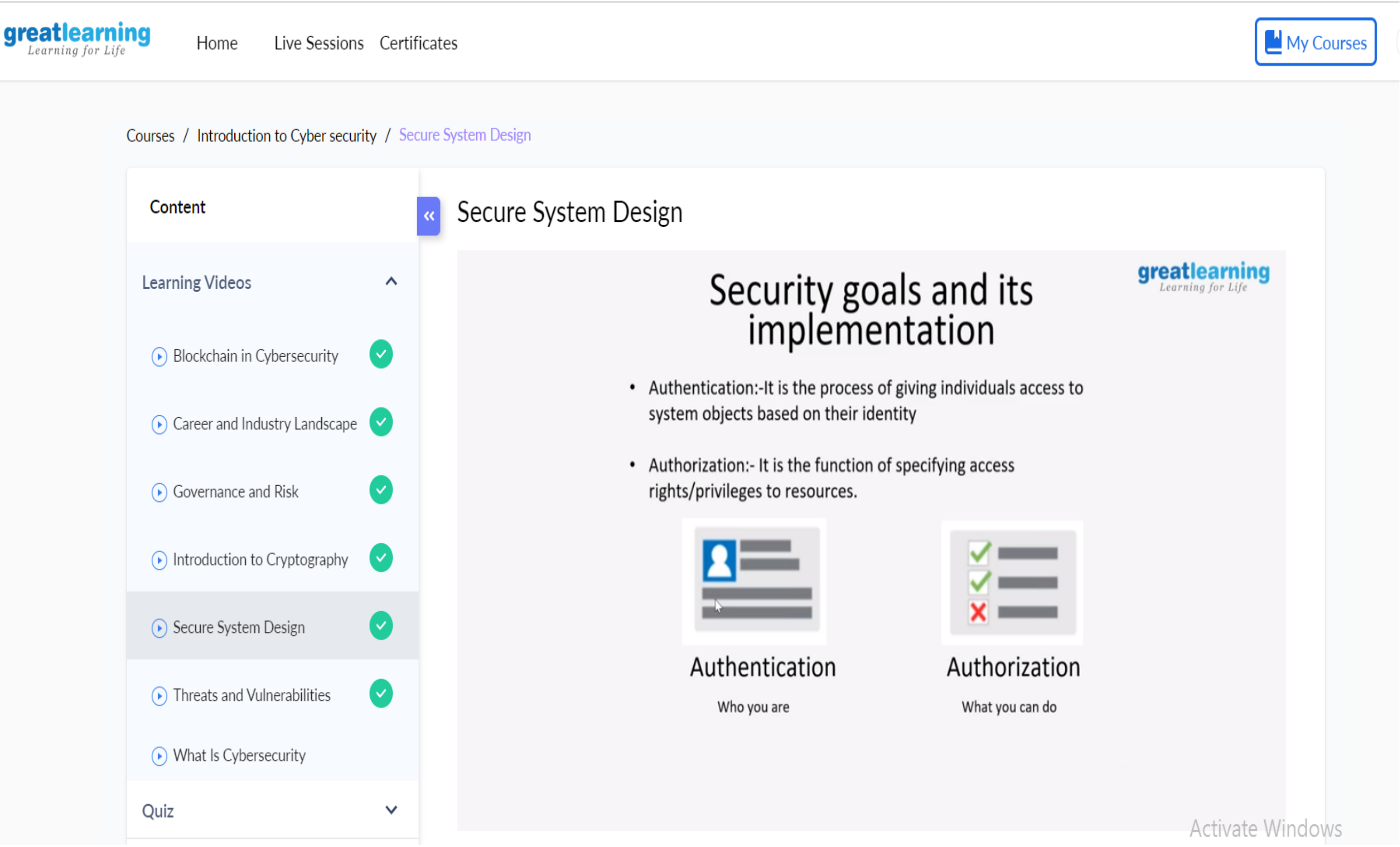
Provided by

Great Learning Academy

(On May 2020)

To verify this certificate visit verify.greatlearning.in/NRYREXMJ

B) Introduction to Cyber Security:


greatlearning
Learning for Life
Home
Live Sessions
Certificates
My Courses
Courses / Introduction to Cyber security / Secure System Design
Content
«
Learning Videos
Blockchain in Cybersecurity
Career and Industry Landscape
Governance and Risk
Introduction to Cryptography
Secure System Design
Threats and Vulnerabilities
What Is Cybersecurity
Quiz
Activate Windows

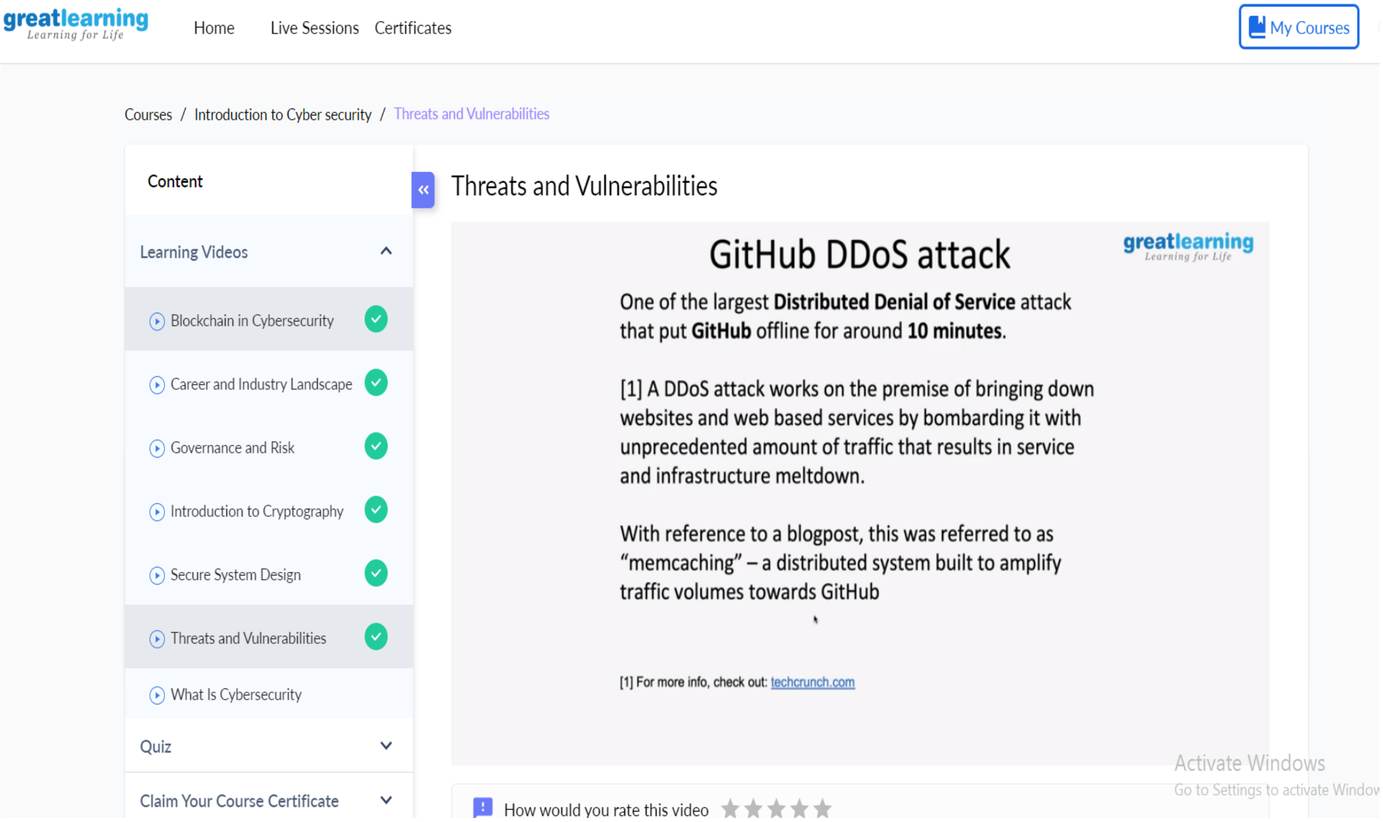
Secure System Design

Security goals and its implementation

- Authentication:-It is the process of giving individuals access to system objects based on their identity
- Authorization:- It is the function of specifying access rights/privileges to resources.

We have divided each set of principles into five categories, loosely aligned with stages at which an attack can be mitigated:

- **Establish the context**
  Determine *all* the elements which compose your system, so your defensive measures will have no blind spots.
- **Making compromise difficult**
  An attacker can only target the parts of a system they can reach. Make your system as difficult to penetrate as possible
- **Making disruption difficult**
  Design a system that is resilient to denial of service attacks and usage spikes
- **Making compromise detection easier**
  Design your system so you can spot suspicious activity as it happens and take necessary action
- **Reducing the impact of compromise**
  If an attacker succeeds in gaining a foothold, they will then move to exploit your system. Make this as difficult as possible


greatlearning Learning for Life
Home
Live Sessions
Certificates
My Courses
Courses / Introduction to Cyber security / Threats and Vulnerabilities
Content
Learning Videos
Blockchain in Cybersecurity
Career and Industry Landscape
Governance and Risk
Introduction to Cryptography
Secure System Design
Threats and Vulnerabilities
What Is Cybersecurity
Quiz
Claim Your Course Certificate
Activate Windows
Go to Settings to activate Window
How would you rate this video ★★★★★

Threats and Vulnerabilities

GitHub DDoS attack

One of the largest **Distributed Denial of Service** attack that put **GitHub** offline for around **10 minutes**.

[1] A DDoS attack works on the premise of bringing down websites and web based services by bombarding it with unprecedented amount of traffic that results in service and infrastructure meltdown.

With reference to a blogpost, this was referred to as "memcaching" – a distributed system built to amplify traffic volumes towards GitHub

[1] For more info, check out: techcrunch.com

Mistakes happen, even in the process of building and coding technology. What's left behind from these mistakes is commonly referred to as a bug. While bugs aren't inherently harmful (except to the potential performance of the technology), many can be taken advantage of by nefarious actors—these are known as vulnerabilities. Vulnerabilities can be leveraged to force software to act in ways it's not intended to, such as gleaning information about the current security defenses in place.

Once a bug is determined to be a vulnerability, it is registered by MITRE as a CVE, or common vulnerability or exposure, and assigned a Common Vulnerability Scoring System (CVSS) score to reflect the potential risk it could introduce to your organization. This central listing of CVEs serves as a reference point for vulnerability scanners.

2) Coding Challenges:

```
#include <iostream>
using namespace std;

int main()
{
        int number = 147; //Any number.
        int res;

        if(number)
                res = number % 9 == 0 ? 9 : number % 9 ;
        else
                res = 0;

        //print the result
        cout<<res;

        return 0;
}
```