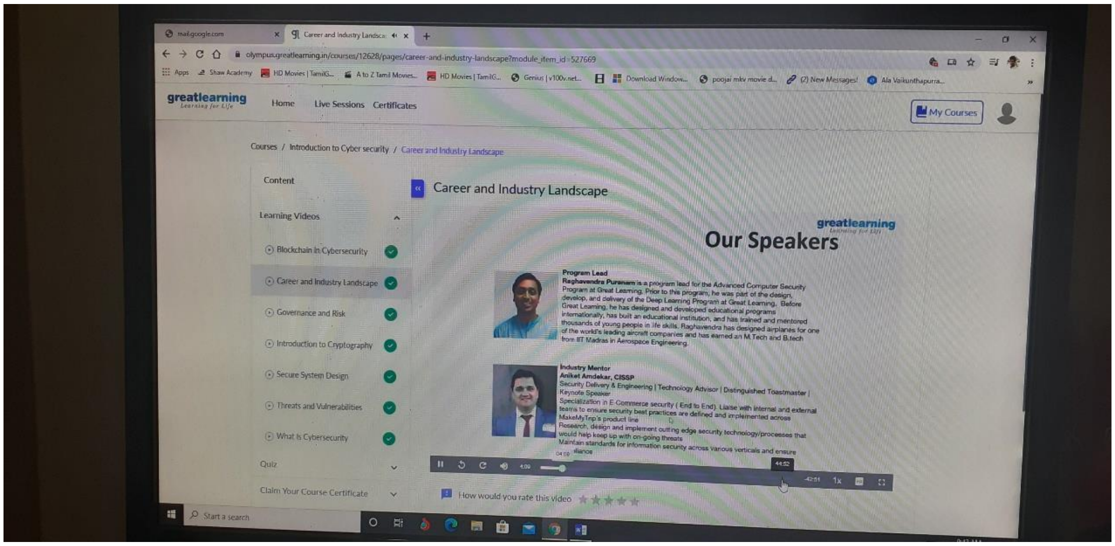
DAILY ASSESSMENT

Date:	**19-6-2020**	**Name:**	**Kavyashree m**
Course:	**Cyber security**	**USN:**	**4al15ec036**
Topic:	**Compliance Governance and industry standards Career, Industry landscape Program relevance**	**Semester & Section:**	**8th A**
GitHub Repository:	**kavya**		

FORENOON SESSION DETAILS



Program Lead
Raghavendra Puranam is a program lead for the Advanced Computer Security Program at Great Learning. Prior to this program, he was part of the design, develop, and delivery of the Deep Learning Program at Great Learning. Before Great Learning, he has designed and developed educational programs internationally, has built an educational institution, and has trained and mentored thousands of young people in life skills. Raghavendra has designed airplanes for one of the world's leading aircraft companies and has earned an M.Tech and B.tech from IIT Madras in Aerospace Engineering.

Industry Mentor
Aniket Amdekar, CISSP
Security Delivery & Engineering | Technology Advisor | Distinguished Toastmaster | Keynote Speaker
Specialization in E-Commerce security (End to End). Liaise with internal and external teams to ensure security best practices are defined and implemented across MakeMyTrip's product line
Research, design and implement cutting edge security technology/processes that would help keep up with on-going threats
Maintain standards for information security across various verticals and ensure [illegible]liance

Compliance Governance

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.

Compliance

Linked directly to governance, compliance helps establish the policies, standards and security controls it will be monitored by. Alongside the reports generated by control monitoring, you must be proactively reassessing your security capabilities and ensuring they are meeting the needs of your business. This means automating application security testing and vulnerability scans, conducting self-assessments from sampling of controls, as well as being overly critical of minute changes, red flags and events that could pose significant risk.

Furthermore, you must also be willing to adapt your processes in response to events and changes to risk. As the sophistication of threats evolve, so should your security posture. Integrating your security operations with the compliance team for response management is key to this, as is establishing standard operating procedures to respond to unintentional changes

Governance

To establish base governance, it’s vital to first identify compliance requirements. This means investigating and understanding contract obligations, compliance frameworks and identifying required or chosen standards that need to be implemented.

Following this, you must conduct a program assessment to understand the capabilities and maturity of your current profile, determine what your target profile is, and create a plan for how you will achieve this. Your strategy should consider procurement, DevSecOps, management, security and human resource allocation, including defining and assigning functions, roles, and responsibilities.

Finally, you need to update and publish your new policies, processes, procedures to educate your employees and reassure that cybersecurity and governance is upheld. Your policies should clearly align with your business objectives. While your processes must specify how to upgrade old technologies for the adoption of modern organization and management techniques, and how your procedures integrate cloud services and other emerging technologies.

Industry standards Career

Organizations across industries are responding by bolstering their cyber defenses and opening more cybersecurity jobs. While salary varies by position, location, and industry, the BLS reports that security analysts earned an annual mean wage of $98,350 in May 2018. Many cybersecurity jobs require at least a bachelor's degree in computer science, information security, or a related field. Some employers may prefer a master's degree.

In these cybersecurity career pages, readers can find a wealth of information about potential career paths, including detailed cybersecurity job descriptions, salary data, and job requirements. In an evolving field with a variety of job options, aspiring cybersecurity professionals should conduct careful research to select a potential career path. Researching cybersecurity jobs can help individuals make the right choices in terms of degree, certifications, and entry-level experience. Cyberattacks cause expensive headaches for companies across industries, including hospitality, healthcare, and insurance. Hackers exploit security weaknesses to collect private information such as social security and credit card numbers, medical data, passwords, and company secrets. Hackers then sell this information to the highest bidder or ransom it back to the company from which they stole it. According to a 2016 Forbes report, industries particularly vulnerable to cyberattacks include healthcare, manufacturing, financial services, government, and transportation. Forbes also highlighted increasing threats to the energy industry.

For high-level positions such as CISO, cybersecurity professionals need 7-10 years of experience. Oftentimes, employers require managers and directors to hold a master's degree. Because cybersecurity degrees teach students proficiency in critical hard skills such as computer programming and network configuration, even entry-level jobs require a bachelor's degree. Some employers seek candidates with a master's degree. Typically, cybersecurity professionals begin in junior positions and advance with years of experience. Through a cybersecurity degree, students hone skills in network and security applications, information systems security, IT security planning and risk management, and ethical hacking. Many employers also seek further professional certifications. Some cybersecurity programs offer pathways to obtaining these credentials.

Industry landscape Program relevance

Industrial sector involves the extraction of resources directly from the earth and the businesses involved in the processing of such products. In the western United States, this pertains to forestry production, fisheries, mining, energy production, and other natural-recourse based businesses.

Landscape: The term ‘landscape’ may describe settlement patterns, infrastructure, and culture alongside the more familiar themes of nature and environment.

Industry analysis and competition

Competition within an industry is grounded in its underlying economic structure. It goes beyond the behavior of current competitors.

The state of competition in an industry depends upon five basic competitive forces. The collective strength of these forces determines profit potential in the industry. Profit potential is measured
in terms of long-term return on invested capital. Different industries have different profit potential just as the collective strength of the five forces differs between industries.

Industry analysis as a tool to develop a competitive strategy

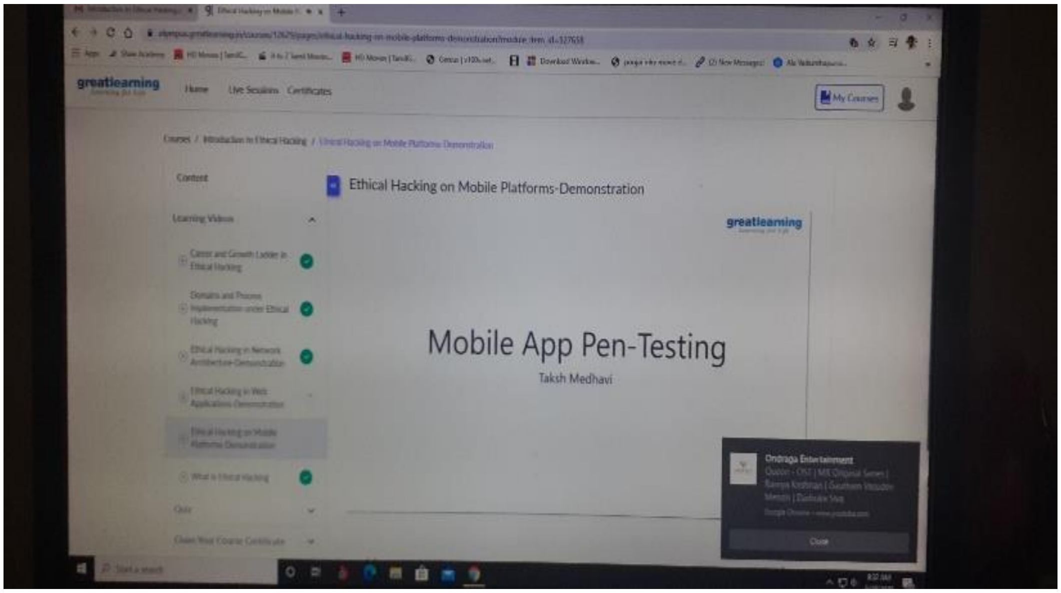
Industry analysis enables a company to develop a competitive strategy that best defends against the competitive forces or influences them in its favor. The key to developing a competitive strategy is to understand the sources of the competitive forces. By developing an understanding of these competitive forces, the company can:

- Highlight the company’s critical strengths and weaknesses (SWOT analysis)
- Animate its position in the industry
- Clarify areas where strategic changes will result in the greatest payoffs
- Emphasize areas where industry trends indicate the greatest significance as either opportunities or threats

AFTERNOON SESSION DETAILS

Date:	**19-6-2020**	**Name:**	**Kavyashree m**
Course:	**Ethical hacking**	**USN:**	**4al15ec036**
Topic:	**Ethical hacking on mobile platforms – Demonstration, Ethical hacking in network architecture - Demonstration**	**Semester & Section:**	**8th A**
Github Repository:	**kavya**		

Image of session



Ethical Hacking on Mobile Platforms-Demonstration

Mobile App Pen-Testing

Taksh Medhavi

greatlearning
Home
Live Sessions
Certificates
My Courses
Content
Learning Videos
Career and Growth Ladder in Ethical Hacking
Domains and Process Implementation under Ethical Hacking
Ethical Hacking in Network Architecture-Demonstration
Ethical Hacking in Web Applications-Demonstration
Ethical Hacking on Mobile Platforms-Demonstration
What is Ethical Hacking
Quiz
greatlearning
Ondraga Entertainment
Close

Ethical hacking on mobile platforms

Mobile devices are used for our most sensitive transactions, including email, banking, and social media. But they have a unique set of vulnerabilities, which hackers are all too willing to exploit. Security professionals need to know how to close the gaps and protect devices, data, and users from attacks. Join author Malcolm Shore as he explores the two dominant mobile operating systems, Android and iOS, and shows ways to protect devices through analysis and testing. Watch this course to review the basics of mobile OS models, the toolsets you need for testing, and the techniques for detecting and preventing the majority of security flaws.

There is no doubt that the demonstration served the objective of sensitizing the audience about the risk of a malware getting installed in their mobile either through the physical access to the phone made available to a hacker or through a malicious link being opened by the mobile user.

The risk of a "Virus" or a "Trojan" in any computer device is already well known. Whether it can be installed in 20 seconds or more or less depends on the size of the file to be installed and the bandwidth of the internet connectivity.

It is therefore not surprising at all to note that Mobiles have a security risk. In fact every electronic device including the EVMs and Aadhar Biometric Devices have risks that we need to recognize. It is for this reason that the Election Commission refused the request of AAP that the EVMs should be handed over to them to show that it is hackable.

What we need to analyze is how to mitigate such risks. In this respect the Saket's demonstration fell short of my expectations.

Normally apps are downloaded from the Google Play Store or Apple Store. In such cases, it is presumed that apps are screened before they are allowed to be uploaded into the Play Store so that malicious apps can be filtered out. However, except identifying the app with a signature of the app creator as declared (which can be an anonymous or pseudonymous) the app store does little to "Certify the App" as "Reliable".

Before the App is installed, it asks for certain permissions and if the permissions are not given, the app may not get installed.

The app needs some permissions depending on its functionality. However, most apps simply get access to several services in the phone and there is no way Google or Apple may know how the permission would be used subsequently when they allow apps to be uploaded into their stores.

Whether an App is asking for only such permissions that it does require for delivering the services it is supposed to provide and not more is a matter which an ordinary user is unable to find out. At the time of downloading the App he is only interested in using the App and hence he will provide permissions to all services sought by the App.

Some Apps may require what is called “Root Access”. This is normally used when some basic hardware functions need to be tweaked by the App. Most manufacturers block root access by design and void their warranty if this block is removed. Most hackers therefore try to work within the non-root access requiring permissions.

When an app is downloaded from a source other than the Play Store, it would be necessary to provide additional “Permission to install from unknown sources” by going to “settings”. (unless it has already been in the open status). Obviously, in this case one has to trust the site from which the app is being downloaded and there would be no assurance from the Play Store about any aspect of the app.

Ethical hacking in network architecture – Demonstration

NMAP

Nmap stands for Network Mapper. It is an open source tool that is used widely for network discovery and security auditing. Nmap was originally designed to scan large networks, but it can work equally well for single hosts. Network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

Nmap uses raw IP packets to determine −

- what hosts are available on the network,
- what services those hosts are offering,
- what operating systems they are running on,
- what type of firewalls are in use, and other such characteristics?

Nmap runs on all major computer operating systems such as Windows, Mac OS X, and Linux.

Metasploit

Metasploit is one of the most powerful exploit tools. It’s a product of Rapid7 and most of its resources can be found at: www.metasploit.com. It comes in two versions − commercial and free edition. Metasploit can be used with command prompt or with Web UI.

With Metasploit, you can perform the following operations −

- Conduct basic penetration tests on small networks
- Run spot checks on the exploitability of vulnerabilities
- Discover the network or import scan data
- Browse exploit modules and run individual exploits on hosts

Burp Suit

Burp Suite is a popular platform that is widely used for performing security testing of web applications. It has various tools that work in collaboration to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.

Burp is easy to use and provides the administrators full control to combine advanced manual techniques with automation for efficient testing. Burp can be easily configured and it contains features to assist even the most experienced testers with their work.

Angry IP Scanner

Angry IP scanner is a lightweight, cross-platform IP address and port scanner. It can scan IP addresses in any range. It can be freely copied and used anywhere. In order to increase the scanning speed, it uses multithreaded approach, wherein a separate scanning thread is created for each scanned IP address.

Angry IP Scanner simply pings each IP address to check if it's alive, and then, it resolves its hostname, determines the MAC address, scans ports, etc. The amount of gathered data about each host can be saved to TXT, XML, CSV, or IP-Port list files. With help of plugins, Angry IP Scanner can gather any information about scanned IPs.

Cain & Abel

Cain & Abel is a password recovery tool for Microsoft Operating Systems. It helps in easy recovery of various kinds of passwords by employing any of the following methods −

- sniffing the network,
- cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks,
- recording VoIP conversations,
- decoding scrambled passwords,
- recovering wireless network keys,
- revealing password boxes,
- uncovering cached passwords and analyzing routing protocols.

Cain & Abel is a useful tool for security consultants, professional penetration testers and everyone else who plans to use it for ethical reasons.

Ettercap

Ettercap stands for Ethernet Capture. It is a network security tool for Man-in-the-Middle attacks. It features sniffing of live connections, content filtering on the fly and many other interesting tricks. Ettercap has inbuilt features for network and host analysis. It supports active and passive dissection of many protocols.

You can run Ettercap on all the popular operating systems such as Windows, Linux, and Mac OS X.

Ether Peek

Ether Peek is a wonderful tool that simplifies network analysis in a multiprotocol heterogeneous network environment. Ether Peek is a small tool (less than 2 MB) that can be easily installed in a matter of few minutes.

Ether Peek proactively sniffs traffic packets on a network. By default, Ether Peek supports protocols such as AppleTalk, IP, IP Address Resolution Protocol (ARP), NetWare, TCP, UDP, NetBEUI, and NBT packets.

Super Scan

Super scan is a powerful tool for network administrators to scan TCP ports and resolve hostnames. It has a user friendly interface that you can use to −

- Perform ping scans and port scans using any IP range.
- Scan any port range from a built-in list or any given range.
- View responses from connected hosts.
- Modify the port list and port descriptions using the built in editor.
- Merge port lists to build new ones.
- Connect to any discovered open port.
- Assign a custom helper application to any port.

QualysGuard

QualysGuard is an integrated suite of tools that can be utilized to simplify security operations and lower the cost of compliance. It delivers critical security intelligence on demand and automates the full spectrum of auditing, compliance and protection for IT systems and web applications.

QualysGuard includes a set of tools that can monitor, detect, and protect your global network.

Web Inspect

Web Inspect is a web application security assessment tool that helps identify known and unknown vulnerabilities within the Web application layer.

It can also help check that a Web server is configured properly, and attempts common web attacks such as parameter injection, cross-site scripting, directory traversal, and more.

LC4

LC4 was formerly known as L0phtCrack. It is a password auditing and recovery application. It is used to test password strength and sometimes to recover lost Microsoft Windows passwords, by using dictionary, brute-force, and hybrid attacks.

LC4 recovers Windows user account passwords to streamline migration of users to another authentication system or to access accounts whose passwords are lost.

LANguard Network Security Scanner

LANguard Network Scanner monitors a network by scanning connected machines and providing information about each node. You can obtain information about each individual operating system.

It can also detect registry issues and have a report set up in HTML format. For each computer, you can list the NetBIOS name table, current logged-on user, and Mac address.

Network Stumble

Network stumble is a Wi-Fi scanner and monitoring tool for Windows. It allows network professionals to detect WLANs. It is widely used by networking enthusiasts and hackers because it helps you find non-broadcasting wireless networks.

Network Stumble can be used to verify if a network is well configured, its signal strength or coverage, and detect interference between one or more wireless networks. It can also be used to non-authorized connections.

ToneLoc

ToneLoc stands for Tone Locator. It was a popular war dialing computer program written for MS-DOS in the early 90’s. War dialing is a technique of using a modem to automatically scan a list of telephone numbers, usually dialing every number in a local area code.

Malicious hackers use the resulting lists in breaching computer security - for guessing user accounts, or locating modems that might provide an entry-point into computer or other electronic systems.

It can be used by security personnel to detect unauthorized devices on a company’s telephone network.