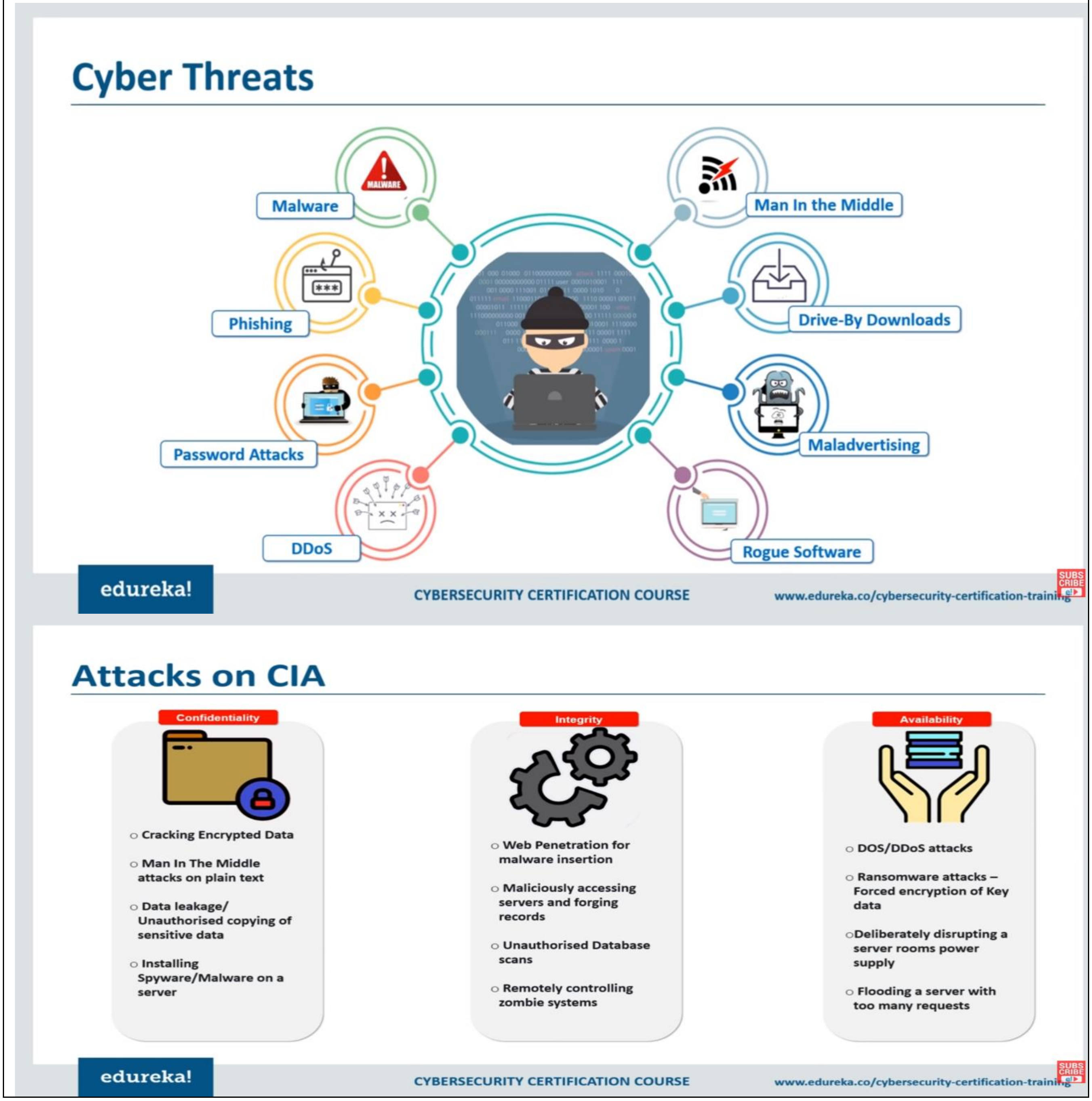
DAILY ASSESSMENT FORMAT

Date:	19th June 2020	**Name:**	Soundarya NA
Course:	Cyber security	**USN:**	4AL16EC077
Topic:	Cyber security	**Semester & Section:**	8th - B

FORENOON SESSION DETAILS

Image of session



Cyber Threats

Malware

Phishing

Password Attacks

DDoS

Man In the Middle

Drive-By Downloads

Maladvertising

Rogue Software

edureka!

CYBERSECURITY CERTIFICATION COURSE

www.edureka.co/cybersecurity-certification-training

Attacks on CIA

Confidentiality

- Cracking Encrypted Data
- Man In The Middle attacks on plain text
- Data leakage/ Unauthorised copying of sensitive data
- Installing Spyware/Malware on a server

Integrity

- Web Penetration for malware insertion
- Maliciously accessing servers and forging records
- Unauthorised Database scans
- Remotely controlling zombie systems

Availability

- DOS/DDoS attacks
- Ransomware attacks – Forced encryption of Key data
- Deliberately disrupting a server rooms power supply
- Flooding a server with too many requests

edureka!

CYBERSECURITY CERTIFICATION COURSE

www.edureka.co/cybersecurity-certification-training

Report:

Compliance:

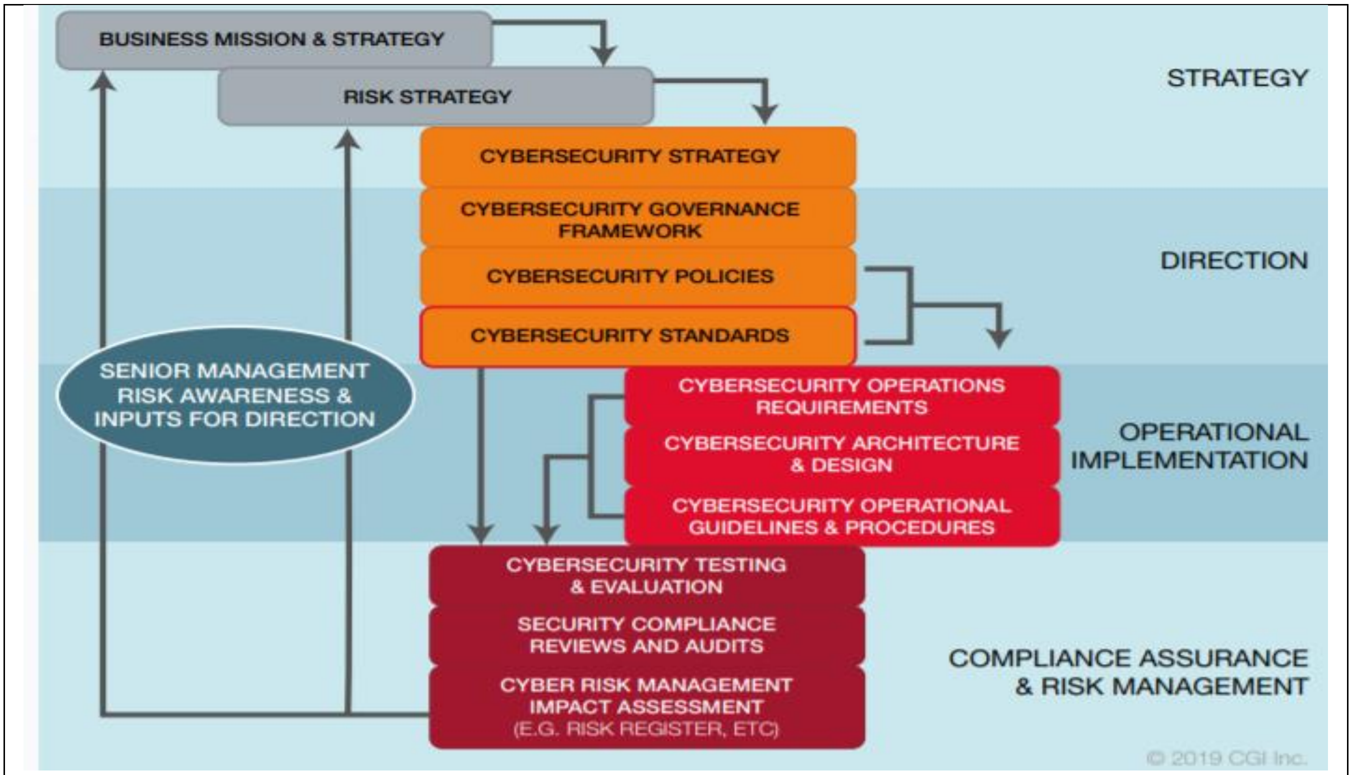
In general, compliance is defined as following rules and meeting requirements. In cybersecurity, compliance means creating a program that establishes risk-based controls to protect the integrity, confidentiality, and accessibility of information stored, processed, or transferred.

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.

Governance and industry standards:

Cybersecurity standards represent a key step in the IT governance process. As a means for managing and containing risk to acceptable levels, the standards must be wholly consistent with IT governance instruments and closely aligned with and driven by the enterprise’s cybersecurity policies. The diagram below represents the typical elements of an IT governance hierarchy. Cybersecurity standards sit at the critical interface between the Direction elements and the Operational Implementation elements. Standards provide essential direction for the objectives and outcomes to be achieved through subsequent implementation activities, such as the development of functional and technical requirements, architecture and design, operational guidelines and operating procedures.


BUSINESS MISSION & STRATEGY
RISK STRATEGY
STRATEGY
CYBERSECURITY STRATEGY
CYBERSECURITY GOVERNANCE FRAMEWORK
CYBERSECURITY POLICIES
CYBERSECURITY STANDARDS
DIRECTION
SENIOR MANAGEMENT RISK AWARENESS & INPUTS FOR DIRECTION
CYBERSECURITY OPERATIONS REQUIREMENTS
CYBERSECURITY ARCHITECTURE & DESIGN
CYBERSECURITY OPERATIONAL GUIDELINES & PROCEDURES
OPERATIONAL IMPLEMENTATION
CYBERSECURITY TESTING & EVALUATION
SECURITY COMPLIANCE REVIEWS AND AUDITS
CYBER RISK MANAGEMENT IMPACT ASSESSMENT (E.G. RISK REGISTER, ETC)
COMPLIANCE ASSURANCE & RISK MANAGEMENT
© 2019 CGI Inc.

Cybersecurity Standards in the IT Governance Hierarchy

Throughout all steps of the IT governance process, direct traceability is needed to ensure effective management, audit and compliance. Cybersecurity standards must reflect, and be crossreferenced to, both the enterprise's policies and its external regulatory obligations (e.g. external standards and controls, such as financial or privacy regulations).

Career and industry landscape:

- Demand for generalist job roles relating to cybersecurity is fading off gradually and being replaced by specialized roles. Demand for artificial intelligence, IT Security forensics, and IoT security skills continue to rise as the industry takes a more pre-emptive approach
- Regulated industries like financial institutions, government operations, retail trade, energy, healthcare, are among those with higher career prospects in the cyber security field. This is due to the legal security regulations that bind their operations thanks in part to the fact that they handle massive consumer information
- Cloud security is among the IT security fields with high demand as more data and operations move to both public and private cloud platforms. Much as the security of cloud services was

vested on the service providers, more industry players are joining the bandwagon to address the security matter as a whole

- While it is possible to opt into the information security without a strong educational background, the job market values education and experience. 84% of employers will set a bachelor's degree, particularly in Information technology or computer science, and at least three years of industry experience as the minimum requirement of their job postings
- After the education qualification and work experience, 35% of employers are likely to use certifications as a criterion for acquiring the best skills
- Employers are already warming up to the idea of including security clearance in their list of requirements. 10% of cybersecurity posts need a security clearance. 10% of these roles, however, take time to be filled
- With the Fortune 500 companies setting the pace, the information security employment landscape is transforming rapidly as more women take up senior positions. It was projected that by 2019, 20% of the CISO roles in Fortune 500 companies would be filled by women in a bid to embrace a gender-inclusive culture in the industry

Program Relevance:

Just as defensive driving improves the safety of other motorists on the road, or staying home when you're sick prevents spreading the flu around your office, maintaining proper cyber security measures on your own devices affects the rest of the online community. As Forbes magazine reports,

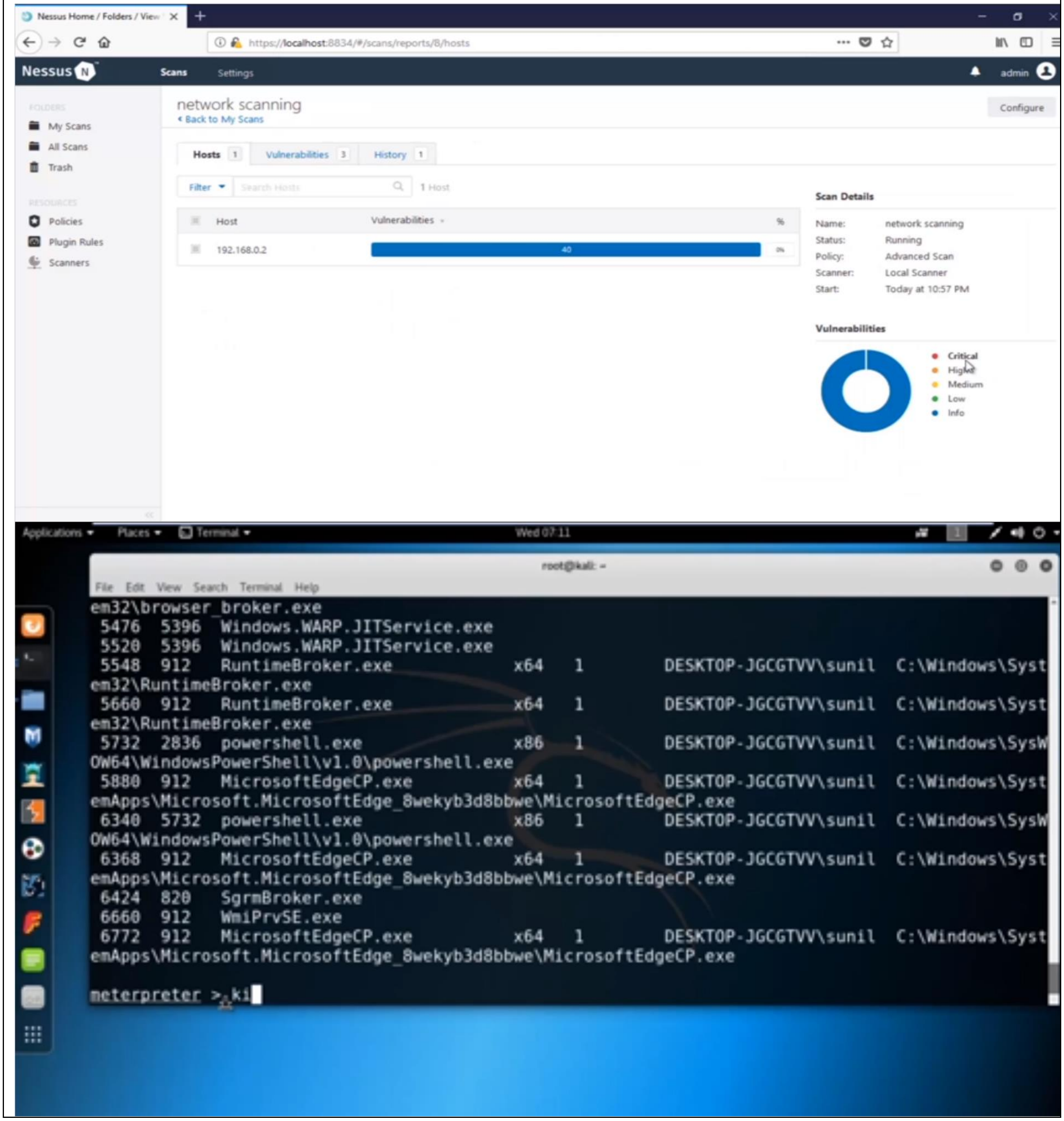
Infected devices have a way of infecting other devices and compromised systems can make everyone vulnerable.

One of the most important groups to teach about cyber security is our youth. While they may not be banking or using credit cards to shop online, they can make it very easy for cyber criminals to access data through creating insecure personal accounts.

Weak passwords and bad practices in email or social media make it much easier for others to hack into your account and gain access to your friends' and family's data. Whether it's a bank account number, a photo best kept private, or complete identity theft, no one wants to be responsible for cybercrime on their loved ones.

AFTERNOON SESSION			
Date:	19th June 2020	**Name:**	Soundarya NA
Course:	Great learning	**USN:**	4AL16EC077
Topic:	Ethical hacking	**Semester & Section:**	8th - B

Image:



network scanning

1 Host

Host	Vulnerabilities	%
192.168.0.2	40	0%

Scan Details

Name: network scanning
Status: Running
Policy: Advanced Scan
Scanner: Local Scanner
Start: Today at 10:57 PM

Vulnerabilities

```
em32\browser_broker.exe
 5476  5396  Windows.WARP.JITService.exe
 5520  5396  Windows.WARP.JITService.exe
 5548  912   RuntimeBroker.exe           x64   1        DESKTOP-JGCGTVV\sunil  C:\Windows\Syst
em32\RuntimeBroker.exe
 5660  912   RuntimeBroker.exe           x64   1        DESKTOP-JGCGTVV\sunil  C:\Windows\Syst
em32\RuntimeBroker.exe
 5732  2836  powershell.exe              x86   1        DESKTOP-JGCGTVV\sunil  C:\Windows\SysW
OW64\WindowsPowerShell\v1.0\powershell.exe
 5880  912   MicrosoftEdgeCP.exe         x64   1        DESKTOP-JGCGTVV\sunil  C:\Windows\Syst
emApps\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\MicrosoftEdgeCP.exe
 6340  5732  powershell.exe              x86   1        DESKTOP-JGCGTVV\sunil  C:\Windows\SysW
OW64\WindowsPowerShell\v1.0\powershell.exe
 6368  912   MicrosoftEdgeCP.exe         x64   1        DESKTOP-JGCGTVV\sunil  C:\Windows\Syst
emApps\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\MicrosoftEdgeCP.exe
 6424  820   SgrmBroker.exe
 6660  912   WmiPrvSE.exe
 6772  912   MicrosoftEdgeCP.exe         x64   1        DESKTOP-JGCGTVV\sunil  C:\Windows\Syst
emApps\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\MicrosoftEdgeCP.exe

meterpreter > ki
```

Report:

Ethical Hacking in mobile platforms:

SEC575 Now Covers Android 10 and iOS 13:

SEC575: Mobile Device Security and Ethical Hacking is designed to give you the skills to understand the security strengths and weaknesses of Apple iOS and Android devices. Mobile devices are no longer a convenience technology - they are an essential tool carried or worn by users worldwide, often displacing conventional computers for everyday enterprise data needs. You can see this trend in corporations, hospitals, banks, schools, and retail stores across the world. Users rely on mobile devices more today than ever before -- we know it, and the bad guys do too. The SEC575 course examines the full gamut of these devices.

Learn How to Pen Test the Biggest Attack Surface in Your Entire Organization:

With the skills you learn in SEC575, you will be able to evaluate the security weaknesses of built-in and third-party applications. You'll learn how to bypass platform encryption and manipulate apps to circumvent client-side security techniques. You'll leverage automated and manual mobile application analysis tools to identify deficiencies in mobile app network traffic, file system storage, and inter-app communication channels. You'll safely work with mobile malware samples to understand the data exposure and access threats affecting Android and iOS, and you'll bypass lock screen to exploit lost or stolen devices.

Take a Deep Dive into Evaluating Mobile Apps and Operating Systems and Their Associated Infrastructures:

Understanding and identifying vulnerabilities and threats to mobile devices is a valuable skill, but it must be paired with the ability to communicate the associated risks. Throughout the course, you'll review ways to effectively communicate threats to key stakeholders. You'll leverage tools, including Mobile App Report Cards, to characterize threats for managers and decision-makers, while also identifying sample code and libraries that developers can use to address risks for in-house applications.

Your Mobile Devices are Going to Come Under Attack - Help Your Organization Prepare for the Onslaught:

In employing your newly learned skills, you'll apply a step-by-step mobile device deployment penetration test. Starting with gaining access to wireless networks to implement man-in-the-middle attacks and finishing with mobile device exploits and data harvesting, you'll examine each step of the test with hands-on exercises, detailed instructions, and tips and tricks learned from hundreds of successful penetration tests. By building these skills, you'll return to work prepared to conduct your own test, and you'll be better informed about what to look for and how to review an outsourced penetration test.

Mobile device deployments introduce new threats to organizations, including advanced malware, data leakage, and the disclosure to attackers of enterprise secrets, intellectual property, and personally identifiable information assets. Further complicating matters, there simply are not enough people with the security skills needed to identify and manage secure mobile phone and tablet deployments. By completing this course, you'll be able to differentiate yourself as someone prepared to evaluate the security of mobile devices, effectively assess and identify flaws in mobile applications, and conduct a mobile device penetration test - all critical skills to protect and defend mobile device deployments.

Ethical Hacking in network architecture:

Hacking has been a part of computing for almost five decades and it is a very broad discipline, which covers a wide range of topics. The first known event of hacking had taken place in 1960 at MIT and at the same time, the term "Hacker" was originated.

Hacking is the act of finding the possible entry points that exist in a computer system or a computer network and finally entering into them. Hacking is usually done to gain unauthorized access to a computer system or a computer network, either to harm the systems or to steal sensitive information available on the computer.

Hacking is usually legal as long as it is being done to find weaknesses in a computer or network system for testing purpose. This sort of hacking is what we call Ethical Hacking.

A computer expert who does the act of hacking is called a "Hacker". Hackers are those who seek knowledge, to understand how systems operate, how they are designed, and then attempt to play with these systems.

Advantages of Hacking:

Hacking is quite useful in the following scenarios −

- To recover lost information, especially in case you lost your password
- To perform penetration testing to strengthen computer and network security
- To put adequate preventative measures in place to prevent security breaches
- To have a computer system that prevents malicious hackers from gaining access

Disadvantages of Hacking:

Hacking is quite dangerous if it is done with harmful intent. It can cause −

- Massive security breach
- Unauthorized system access on private information
- Privacy violation
- Hampering system operation
- Denial of service attacks
- Malicious attack on the system

Purpose of Hacking:

There could be various positive and negative intentions behind performing hacking activities. Here is a list of some probable reasons why people indulge in hacking activities −

- Just for fun
- Show-off
- Steal important information
- Damaging the system
- Hampering privacy
- Money extortion
- System security testing
- To break policy compliance

Hacker types:

Hackers can be classified into different categories such as white hat, black hat, and grey hat, based on their intent of hacking a system. These different terms come from old Spaghetti Westerns, where the bad guy wears a black cowboy hat and the good guy wears a white hat.

White Hat Hackers:

White Hat hackers are also known as Ethical Hackers. They never intent to harm a system, rather they try to find out weaknesses in a computer or a network system as a part of penetration testing and vulnerability assessments.

Ethical hacking is not illegal and it is one of the demanding jobs available in the IT industry. There are numerous companies that hire ethical hackers for penetration testing and vulnerability assessments.

Black Hat Hackers:

Black Hat hackers, also known as crackers, are those who hack in order to gain unauthorized access to a system and harm its operations or steal sensitive information.

Black Hat hacking is always illegal because of its bad intent which includes stealing corporate data, violating privacy, damaging the system, blocking network communication, etc.

Grey Hat Hackers:

Grey hat hackers are a blend of both black hat and white hat hackers. They act without malicious intent but for their fun, they exploit a security weakness in a computer system or network without the owner's permission or knowledge.

Their intent is to bring the weakness to the attention of the owners and getting appreciation or a little bounty from the owners.

Miscellaneous Hackers:

Apart from the above well-known classes of hackers, we have the following categories of hackers based on what they hack and how they do it −

Red Hat Hackers:

Red hat hackers are again a blend of both black hat and white hat hackers. They are usually on the level of hacking government agencies, top-secret information hubs, and generally anything that falls under the category of sensitive information.

Blue Hat Hackers:

A blue hat hacker is someone outside computer security consulting firms who is used to bug-test a system prior to its launch. They look for loopholes that can be exploited and try to close these gaps. Microsoft also uses the term BlueHat to represent a series of security briefing events.

Elite Hackers:

This is a social status among hackers, which is used to describe the most skilled. Newly discovered exploits will circulate among these hackers.

Script Kiddie:

A script kiddie is a non-expert who breaks into computer systems by using pre-packaged automated tools written by others, usually with little understanding of the underlying concept, hence the term Kiddie.

Neophyte:

A neophyte, "n00b", or "newbie" or "Green Hat Hacker" is someone who is new to hacking or phreaking and has almost no knowledge or experience of the workings of technology and hacking.

Hacktivist:

A hacktivist is a hacker who utilizes technology to announce a social, ideological, religious, or political message. In general, most hacktivism involves website defacement or denialof-service attacks.