DAILY ASSESSMENT REPORT

Date:	19/06/20	Name:	Gaganashree P
Course:	Ethical hacking	USN:	4AL15EC024
Topic:	1. Ethical hacking in network architecture and on mobile platforms	Semester & Section:	8TH & A
Github Repository:	Gaganashree-P		

Afternoon SESSION DETAILS

Image of session

greatlearning
Learning for Life
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
Learning for Life

Ethical Hacking on Mobile Platforms-Demonstration

Mobile App Pen-Testing

Taksh Medhavi

1. Ethical hacking on mobile platforms –Demonstration

Mobile applications are a major point of vulnerability in organizations today. Nex-G Innovations Mobile App Penetration Testing and Ethical Hacking Training Course covers all aspects of Mobile Mobile App Penetration Testing Training and Mobile App Ethical Hacking. Attendees will learn the art of exploiting and penetrating Mobile applications so security and performance flaws can be found in your mobile apps before the real hackers do. Through detailed, hands-on exercises and training from a experienced mobile ethical hacker professional, students will be taught the six-step process for Mobile application penetration testing and explore various other Mobile app vulnerabilities in depth. You will learn the hacking and mitigation tools and methods for the mobile apps used by the attacker, so that you can be a powerful defender yourself.

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.

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.

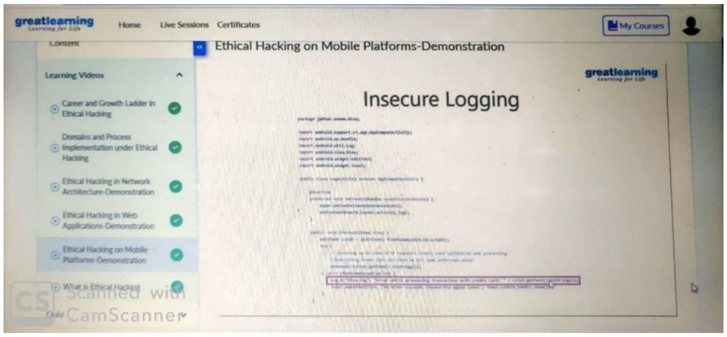
Mobile Ethical Hacking training course was designed and created to introduce mobile device security basic principals, mobile network architecture, mobile app development, policy and enforcement rules, mobile code analysis, penetration testing and mobile ethical hacking.

Mobile hacking is an emerging threat targeting many end users and enterprises. Cybercriminals launch many mobile attacks including mobile phishing attacks since they can take of certain limitations of the mobile platform.

Through the hands-on labs and workshop, students will practice and learn about principals around securing mobile devices, mobile applications and mobile networks. Learn how to analyze and evaluate mobile app threats, mobile device penetration and exploit and how the attackers find out about mobile devices and applications weaknesses.

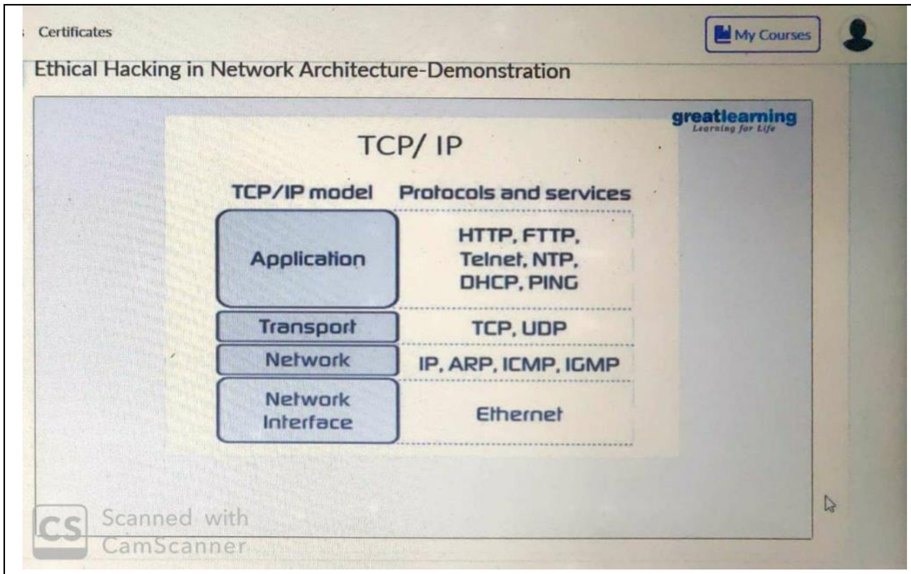
Mobile devices are used for our most sensitive transactions, including email, banking, and social media. But they have a unique set of vulnerabilities, which hackers are all too willing to exploit.

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.


greatlearning
Learning for Life
Home
Live Sessions
Certificates
My Courses
Content
Ethical Hacking on Mobile Platforms-Demonstration
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
Insecure Logging

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. course examines the full gamut of these 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.

2. Ethical hacking in network architecture



Ethical Hacking in Network Architecture-Demonstration

TCP/ IP

TCP/IP model	Protocols and services
Application	HTTP, FTTP, Telnet, NTP, DHCP, PING
Transport	TCP, UDP
Network	IP, ARP, ICMP, IGMP
Network Interface	Ethernet

Certified ethical hackers

There are a number of ethical hacking certifications as well as IT certifications related to security that can help individuals become ethical hackers, including:

Certified Ethical Hacker (CEH): This is a vendor-neutral certification from the EC-Council, one of the leading certification bodies. This security certification, which validates how much an individual knows about network security, is best suited for a penetration tester role. This certification covers more than 270 attacks technologies. Prerequisites for this certification include attending official training offered by the EC-Council or its affiliates and having at least two years of information security-related experience.

Certified Information Systems Auditor (CISA): This certification is offered by ISACA, a nonprofit, independent association that advocates for professionals involved in information security, assurance, risk management and governance. The exam certifies the knowledge and skills of security professionals. To qualify for this certification, candidates must have five years of professional work experience related to information systems auditing, control or security.

Certified information security manager (CISM): CISM is an advanced certification offered by ISACA that provides validation for individuals who have demonstrated the in-depth knowledge and experience required to develop and manage an enterprise information security program. The certification is aimed at information security managers, aspiring managers or IT consultants who support information security program management.

GIAC Security Essentials (GSEC): This certification created and administered by the Global Information Assurance Certification organization is geared toward security professionals who want to demonstrate they are qualified for IT systems hands-on roles with respect to security tasks.

Candidates are required to demonstrate they understand information security beyond simple terminology and concepts.