DAILY ASSESSMENT REPORT

|  |  |  |  |
| --- | --- | --- | --- |
| Date: | 19/06/20 | Name: | Prajna |
| Course: | Ethical hacking | USN: | 4AL16EC047 |
| Topic: | 1. Ethical hacking in network architecture and on mobile platforms | Semester & Section: | 8TH A |
| Github Repository: | prajna\_salian |  |  |

|  |
| --- |
| **Afternoon SESSION DETAILS** |
| **Image of session**      Computer hacking is a practice with many nuances. Intent, whether benign or malicious, is often in the eyes of the beholder. The word hacking is defined as an illegal use of the other’s computer system or the network resources. When examining the root cause of a website hack or application exploit, it pays to follow the money. Hacker is the term which is formerly meant for the skillful programmer. A hacker will be motivated by whomever or whatever is sponsoring his or her actions. The word hacker refers to the names of the persons who enjoys the work in learning the details of the computer systems and stretch the capabilities from the system. The system of hacking describes the fast improvement in the new programs that make the codes for the providing a better security to the system with more efficiency. The word cracker also belongs to the same field it make use of thehacking skills for the unlawful purposes like email id, intruding into other’s system. Hacking is of different types such as back door hacking, viruses and worms, Trojan horses, Denial of Services, anarchists, crackers, kiddies and ethical hacking. In the types of hacking system one of the most common hacking is **ethical hacking**. The computer security industry coined the term “ethical hacking” to describe a hacker who benevolently attacks a network or other security system  – whether private or public – on behalf of its owners. Ethical hackers are also called white hat hackers, as distinguished from the black-hatted bad guys. |
| 1. **Ethical hacking on mobile platforms**   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.  Design and run mobile hacking attacks in the classroom labs. Some of the mobile hacking concepts you will learn to master mobile hacking are:   * Mobile device and application architecture * Mobile and device security functions * Mobile networks ethical hacking * Mobile security and management * Mobile phones, tablets, and applications ethical hacking * Mobile penetration testing * Mobile device threats, policies, and security models and frameworks * Mobile Code and Application Analysis * Techniques and Procedures to Secure Mobile Phone * Mobile application code analysis, architecture and management * Mobile device and application penetration testing methodologies * Mobile passive traffic identification * Remote root vulnerability exploitation on Android and iOS platforms * Mobile privilege escalation hacking * Remote access trojan mobile hacking * Attacking wireless and mobile network infrastructure devices * Hacking by brute forcing remotely * Hiding exploit payloads * TONEX’s mobile security and ethical hacking framework   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.    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.  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.  **2. Ethical hacking in network architecture**    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. |
| **Applications  of Ethical Hacking:** Ethical hacking is nothing but the one which performs the hacks as security tests for their systems. Ethical hacking can be used in many applications in case of web applications which are often beaten down. This generally includes Hypertext Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP) applications are most frequently attacked because most of the firewalls and other security are things has complete access to these programs from the Internet. Malicious software includes viruses and Trojan horses which take down the system. Spam is a junk e-mail which causes violent and needless disturbance on system and storage space and carry the virus, so ethical hacking helps to reveal such attacks against in computer systems and provides the security of the system.  The main application of this is to provide the security on wireless infrastructure which is the main purpose of present business organization. Ethical hacking has become main stream in organizations which are wishing to test their intellectual and technical courage against the underworld. Ethical hacking plays important role in providing security. Resources are the computer related services that performs the tasks on behalf of user. In Ethical hacking the resources are the core services, objects code etc.  The ethical hacking has advantages of gaining access to an organizations network and information systems. This provides the security in the area of Information technology called as Infosec. This provides security to the high level attacks such as viruses and traffic trough a firewall. This has been providing the security for various applications which are even bypassing the firewalls, Intrusion-detection systems and antivirus software. This includes hacking specific applications including coverage of e-mails systems, instant messaging and [VOIP (voice over IP)](https://www.mbaknol.com/information-systems-management/voice-over-internet-protocol-voip/). The resources i.e. devices, systems, and applications that are generally used while performing the hacking process are Routers, Firewalls, Network infrastructure as a whole, wireless access points and bridges, web application and database servers, E-mail and file servers, workstations, laptops and tablet PCs, Mobile devices, client and server operating systems, client and server applications .  Ethical hacking tests both the safety and the security issues of the programs. Hence from the above context it can be stated as the ethical hacking is important in the present scenario as providing security is very important now a day. This is very important in web applications as the hacking can be easily done in this case. |