Chapter 11
Why One Should Learn Ethical Hacking

Sunita Vikrant Dhavale
Defence Institute of Advanced Technology, India

ABSTRACT

This chapter presents the importance of learning hacking techniques by each and every person dealing with cyber operations. The chapter explains various basic terminologies used in the ethical hacking domain and also provides step-by-step instructions for setting up an ethical hacking lab. The chapter also reveals the legal issues with the ethical hacking domain by providing details of existing cyber laws, acts, and regulations framed by various countries in order to deal with the harmful hacking activities and cybercrimes.

INTRODUCTION

"If you know your enemies and know yourself, you will not be imperiled in a hundred battles... if you do not know your enemies nor yourself, you will be imperiled in every single battle"; was quoted precisely by the famous Chinese military General Sun Tzu (Sun Tzu, 2018). Studying attackers and their attack techniques will definitely help us in building effective defense posture for our systems and networks in the cyber space.

As of the most recent reported period, the number of internet users worldwide has increased to 3.58 billion. Access to the internet by users becomes unavoidable with the advent of technological developments and numerous advantages like easy data sharing, collaborative working style, flexibility, low cost, easy access, availability of different cloud computing models, online storage models, social networking, shopping, browsing publicly available data/information etc. As each and every individual or organization/institute has gained a greater online presence, cyber security has become a vital topic of concern (Singer & Allan, 2014). Many individual activities continue to evolve in the cyber space and this increased dependence on cyberspace can escalate vulnerability in one's information assets. The threats from hackers, spies, terrorists, and criminal organizations against our information assets are undeniable. Recently a

DOI: 10.4018/978-1-6684-3554-0.ch011

massive ransom waremalware attack hit many critical servers across the globe including countries like Russia, Ukraine, Romania, the Netherlands, Norway, France, Spain, Britain, US, Australia and India. The attackers used social engineering tools and techniques successfully to exploit these systems by luring the innocent users to download popular tax accounting package or to visit a local news site (Jessica, 2018). The attackers were successful to extort money from some of the computer users. If we don't prepare our self against these attacks in time, the serious consequences like identity theft, theft of sensitive/proprietary information/trade secrets or loss of reputation/credibility in the market; may result. A single malicious attempt can bring down any reputed organization or financial institution to a halt, by causing a great damage may be costing in millions of dollars per hour.

One cannot protect his information assets if he doesn't know how attackers think and what techniques attackers use to exploit systems. Hence, learning offensive security techniques like Ethical Hacking is becoming a need of future cyber security world. Ethical hacking knowledge base can be used for testing/improving network and system security posture of organization. One can identify the security risks and vulnerabilities in a network with the help of ethical hacking knowledge base. There is a need for each individual and institute to learn hacking tools and techniques which are used by these dangerous hackers and to create a cyber-security team including Ethical hacking professionals in order to test their systems effectively (UKEssays, 2018). It's always good to know in prior, if there is any means to gain access to our stored sensitive data; before getting it exploited by the wrong persons. This will help us in protecting our valuable data from getting into wrong hands in this connected cyber world (Arce, & McGraw, 2004).

Before starting, one should keep in mind that there is a difference between learning ethical hacking subject and other traditional network security subjects. In general, traditional system and network security (Bishop, 2004) educational domain generally focus on the topics like network defense, firewalls, intrusion prevention systems (IPS), Intrusion Detection Systems (IDS), Antivirus techniques, Security Policies, Computer Security etc. (Bishop, 2002). while; Ethical Hacking domain focus on attacking the secure or unsecure networks and systems, sniffing transmitted data, password cracking, social engineering attacks, malware generation and all means that can exploit a network and system defense perimeter. Hence the learning approach of ethical hacking subject will be totally different from that of other network security related subjects. The offensive nature of ethical hacking subject makes it different.

Also, traditional cyber security education is based on bottom-up approach where security topics are taught separately in an isolated context, with little effort to link these topics together. Top-down and case-driven (TDCD) teaching model (Cai, & Arney, 2017) can be adopted for teaching offensive cyber security which allows learner to follow the footprints of hackers during the case analysis in order to gain practical experience along with the detailed study on how exploitation of different security mechanisms and weakest links can be achieved by attacker. The case analysis can be based on real-world cyber breaches like the Target Corporation breach, the Anthem Inc. Breach etc. Such case-study based cyber security course teaching models (Cai, 2016) will help one to gain a holistic view of security and to apply multiple defensive techniques in complex contexts by observing the flow of attack and its impact.

BASIC TERMINOLOGIES

Before exploring ethical hacking domain, we would need to know a few basic terms and what they mean.