Chapter 13
Changing Dynamics of Network Security involving Hacking/Cracking with Next Generation Firewalls (NGFW)

Alok Vishwakarma
Sysbiz Technologies, India

Wafa Waheeda S
Qatar University, Qatar

ABSTRACT

With increasing number of users on the internet, risk of security and probability of vulnerable attacks are increasing day by day. For every user connected to network, security attacks like hacking and cracking are very frequent which leaves enormous amounts of sensitive data at the risk of being altered, lost or misused. This apparently leads to the need for security measures on ports and protocols also search for application security, VPN, IPS, and a firewall support. The hacking and cracking threats and attacks in a network are no longer in control with the existing methods and standard firewalls. The introduction of Next Generation Firewalls leads to improved security over network. This chapter deals with hacking and cracking attacks over network and their countermeasures, also focusing on the changing dynamics of network security with next generation firewalls.

INTRODUCTION

Network security has continuous growing necessitate for measures to prevent attacks, data loss and any kind of threat while hacking and cracking being the primary reasons (Negi, 2011). Internet being called the network of networks - empowers people, but also admonishes with restricted access in order to protect the network for having safe access with proper network security measures.

Hacking is unauthorised access to any network or a computer which leads to misuse of information and causes risk to the security of network (Negi, 2011). Whereas Cracking being similar to Hacking,
Changing Dynamics of Network Security involving Hacking/Cracking with NGFW

Hacking and Cracking

Hacking is an intrusion in a computer or network which provides access to authorised or unauthorised data. This is a threat to the network security systems because of the risk factor (Simmonds, Sandilands, & Van Ekert, 2004, p. 317-323). The main objective of hacking is the serious attempts to find the flaws in a system or network, which leads to the risk factor involved.

Hackers break into a system with no intention to harm, rather to gain knowledge, have the interest of fulfilling their curiosity, to try creating different things or even to test their hacking capabilities (Negi, 2011). This might lead a hacker to face legal consequences, but mostly the hacker causes no harm to the system after they hack in. Generally, hacking is to try out new and different things from a system or software which is totally opposite to its usage or its purpose in the first place. But hacking can be ethical and unethical, as there are many types and groups of hackers present. The White Hat Hackers, Grey Hat Hackers and Black Hat Hackers etc. are the groups of hackers present.

Hackers try to attack a system or a server in a network with the many type of hacking attacks, like Denial of Service DOS, Man in the Middle MITM, E-mail Bombing, Spoofing, Phishing etc (Daya, 2013; Dwivedi, 2009; Kessler, Gary C., 2000). The hackers target a particular system by spamming or any kind of attack, and when a user - while clicking on a spammed file or link, a malicious code or program is installed and runs without the knowledge of user. In that way the hacker successfully hacks a user (victim) and controls the victim’s system to hack the server or a network (see Figure 1).

Cracking is malicious as it deals with misuse of information present in the hacked system or network. The main objective of cracking is to steal and misuse the data for own personal reason. This is the most unethical and malicious form of hacking and intrusion, as it involves bad intensions and incorrect usage of hacked system or network’s information (Negi, 2011).

Crackers perform certain type of attacks to exploit the system or network for their own benefit. This includes cracking of licensed software’s and building keygens - key generators a software which helps crack a software licence and run for free. Crackers also crack bank security systems, network security systems etc. They deal with cracking the password with Brute force attack, Dictionary attack etc.
Related Content

Formal Methods for the Development and Verification of Autonomic IT Systems
[www.igi-global.com/chapter/formal-methods-development-verification-autonomic/60442?camid=4v1a](www.igi-global.com/chapter/formal-methods-development-verification-autonomic/60442?camid=4v1a)

Protecting Data Confidentiality in the Cloud of Things

Internet of Things: Privacy and Security Implications
[www.igi-global.com/article/internet-of-things/179894?camid=4v1a](www.igi-global.com/article/internet-of-things/179894?camid=4v1a)

Introduction of Vehicular Network Applications
[www.igi-global.com/chapter/introduction-vehicular-network-applications/39517?camid=4v1a](www.igi-global.com/chapter/introduction-vehicular-network-applications/39517?camid=4v1a)