The Difference Between Hackers and Intruders: Case Study

A. Sh. Ashoor

Department Mathematics –College of Education for Pure Science

University of Babylon - Iraq
asmaa_zaid218@yahoo.com

Abstract:

This paper presents the difference between hackers and intruders with their main motives and intentions with their way of thinking, planning and performing attacks for their personal gain and as well as others gain. This shows the security of computer networks and information systems can't protect effectively if the human factor fails. Here explaining how the network is hacked or intruded by using several numbers of tools with achieving their motives.

Keywords:
Hackers, intruders, security, criminal, network scanning, motives.

Introduction:

The usual way of analysing network security model is using through various technologies like IDS, IPS, firewalls, UTMs, access control lists and malicious software defence etc. To covering all these various technology areas to achieve organizational security with basis of network security architecture, design, policies and procedures. The common goal is to intend this 'acceptable security risk' and to target with network security model by using other security and protections systems.

The hacker is a 'computer criminal' to hack or theft or steals the organization information. The hacker is someone who is mastermind in art of programming to point that he or she simply sit down and hack in a program that works. But the intruders are basically who violate networks and information systems. The intruders are aware of weakness in system and networks through their continuously network scanning programs.

Here in this paper gives the difference between hackers and intruders but their goal is same to violate or theft the information and to break the wall of weaker network security model architectures.

What Hackers means and their motives:

The most common usage of "hacker" is to breakdown computer security without authorization or indeed, usually through a computer network or the internet for terrorism, vandalism, credit card fraud, identity theft, intellectual property theft, and many other forms of crime. This can mean taking control of a remote computer through a network, or software cracking. These hackers are called cracker or black-hat hacker or simply "criminal". But the one who help the government or organization to trace the intrusions of black-hat hacker and break the network or information by criminals called as "Ethical Hacker"

The history of hackers in prior to mid-1980s, was blur, means hacker known only as researchers in universities and corporate research parks. But in 1983 film "War Games" was a boom in home hacking. That time many unfortunately true hackers was popularized also as criminal and disaster in networks.

"The trouble began with some well-publicized arrests of teenagers who electronically ventured into forbidden digital grounds, like government computer systems" (Levy, 1984). These well-publicized arrests included the 414 Gang (from Milwaukee—area code 414). "'414 Private' was the home board for the first *group* to attract conspicuous trouble, the teenage '414 Gang,' whose intrusions into Sloan-Kettering Cancer Center and Los Alamos military computers were to be a nine-days-6 Law Enforcement Training Network wonder in 1982." The other notorious "hacker crackdown" culminated in the Operation Sundevil arrests in 1990 (Sterling, 1992). The original "Old-School" hackers never worried about breaking computer laws because there were none."

In the new generation that assumed "hacker" is defined for beginning by crime only. The modern day hackers have enormously more power available through the internet access, and they are easily breaking the network access by using user-friendly hacking tools.
The hacker motives are classified in three broad categories as

- Recreation: Those who hacks in to network for 'just fun' or to prove their technical powers.
- Remuneration: The people who hack the network for personal gain like attempt to transfer funds in their own bank accounts, 'hackers for hire' as to break the network on paid by others basis.
- Revenge: Dissatisfied customers, disgruntled former employees, angry competitors comes in this category.

What intruder's means and their motives:

A network intruder are gaining access through unauthorised access to networking devices through physical, system and remote attempts. The intruder uses some outdated exploits that are ineffective against up-to-date patched hosts. The intruders are of two types. One is external intruder is an unauthorized user of the system or network, and the internal intruder is an authorized user who has access to certain areas of the internal system or network.

The intruders are basically three forms one 'masquerade user' who is authorized user to use computer, second 'misfeasor' legitimate user who misuse his/her privileges and third 'clandestine user' who seizes his supervisory control of the system and uses it to suppress audit information.

The intruder's main motives are-

- To perform network scanning to find out vulnerable hosts in the network.
- To install an FTP server for distributing illegal content on network (ex. pirated software or movies)
- To use the host as a spam relay to continuous flood in the network
- To establish a web server (non-privileged port) to be used for some phishing scam.

Tools used by Hackers & Intruders:

There are several common tools used by computer criminals to penetrate network as:

- Trojan horse - These are malicious programs or legitimate software is to be used set up a back door in a computer

system so that the criminal can gain access.

- Virus - A virus is a self-replicating program that spreads by inserting copies of itself into other executable code or documents.
- Worm - The worm is a like virus and also a self-replicating program. The difference between a virus and a worm is that a worm does not attach itself to other code.
- Vulnerability scanner – This tool is used by hackers & intruders for quickly check computers on a network for known weaknesses. Hackers also use port scanners. This check to see which ports on a specified computer are "open" or available to access the computer.
- Sniffer – This is an application that captures password and other data in transit either within the computer or over the network.
- Exploit – This is an application to takes advantage of a known weakness.
- Social engineering – Through this to obtain some form of information.
- Root kit - This tool is for hiding the fact that a computer's security has been compromised.

Difference between Intruders and Hackers:

A hacker has a lot of computing skills and challenges of solving technical problems. This includes the failure of computers and networks. But the goal of intruder is no damage of network, the technical aspects and how to overcome as learners and status symbol among the hacker community.

"A hacker is a person who intensely interested in the workings of any computer operating system. The hackers are most often programmers. As such, hackers obtain advanced knowledge of operating systems and programming languages. They might discover holes within systems and the reasons for such holes. Hackers constantly seek further knowledge; freely share what they have discovered, and never intentionally damage data.

The intruder is one who breaks into or otherwise violates the system integrity of remote machines with malicious intent. Having gained unauthorized access, crackers destroy vital data, deny legitimate users service, or cause problems for their targets. Crackers can easily be identified because their actions are malicious."

The difference between hacker and intruder might not seem much to the average person because after all divided into two computers and networks not allowed but that is what matters the person made after he infiltrates a network.

Result achieved and future research:

Through the basic details, classifications and analysis of hackers and intruders, that they trying to violate networks and information systems. The final intention is to mitigate risks and give suggestions and direction for building a security protection system, with using intrusion detection and intrusion prevention systems. There are many difficulties in attempt to make this works to be happen, such as:

- Many of the organizations are not ready to disclose details about their problems they have been experiencing or facing.
- The peoples are not ready to talk openly about their attacks and hackers' exploits and "accomplishments".

- This area requires very often to have good relation to people that are from “grey” zone, what is not so easy and popular.
- There is not any open literature that treats this problem to be resolving completely.

There are many other problems also in this future research related to legal and ethical and similar other issues.

Conclusion:

This paper presented about difference between hackers and intruders. The hackers and intruders have major motives and intention by using various classifications of tools for penetrating the network. The hacker who hacks or theft the information in network for personal gain or any other gain, which classified as black hat hacker and ethical hacker. The intruders are who intrude continuously through network scanning using with sniffers in network for penetrating the network to achieve their motives. The result achieved and future research on intruders and hackers with classification and analysis for violating network and information systems but actually many organizations are not shared their data in case of affecting their systems and networks. This is actual fact to lack in resolving the issues about hackers and intruders.The technical mechanisms and complex technologies can’t assure security and many protection systems fail due to human mistakes and omissions.

References:

1. William Stallings ,”Network securityessentials:applications and standards”, 2010
2. Carl Endorf, Eugene Schultz and Jim Mellander "Intrusion Detection and Prevention";; 2004.
3. Thomas W. Shinder, Debra Littlejohn Shinder, Adrian F. Dimcev, “Dr. Tom Shinder's ISA Server 2006 Migration Guide” .
4. DraganPleskonjic”Psychologi-cal Profile of Network Intruder “.
5. Digital Crime: Hackers, Part 1 -Release date: 12/03
6. Peter Stephenson ,”Computer-Related Crime A handbook for corporate”. By CRC Prss LLC,2000.
7. Handbook of Managing Cisco Network Security
8. Carnegie Mallon, “CERT 2009 Research Report”, softwareEngineering Institute.
9. InformIT,”The difference betweenhackers and crackers” , 2003.