Packet Crafting Tools for Cyber Crime Security Attacks

Prathyusha Kanakam
MVGR College of Engineering
Vizianagaram
Andhra Pradesh, India

ASN Chakravarthy
JNTU Kakinada
Vizianagaram
Andhra Pradesh, India

ABSTRACT
Due to the advancement in the Internet which is coined as the network of networks, there may have a chance to raise a lot of vulnerabilities during the communication of peers that challenge network’s security issue. All the security breaches including firewalls are failed to overcome these vulnerabilities. Packet Crafting is one of all those security attacks. It is the process that changes the information transferred between various peers of the network in a digital manner. In this paper, a detailed report on packet crafting as well as various investigating tools related to this type cyber-crime is presented.

General Terms
Security; Communication; Information; Internet; Cyber Forensics; Investigating tools

Keywords
Cyber-crimes; Cyber-Forensics; Intruder detection; Packet crafting

1. INTRODUCTION
Crimes in this digital world are of different types and the one among is Cyber-crime1. As everything is digitized, there is the rapid increase in the use of Internet and at the same time number of cyber-crimes happens that raised by the attackers. Cyber-crimes involve both computer and network. During the communication over networks, intruder detection is a predictive task for recent issues of research. The statistical studies of 2016 on various network-based attacks reveal that more than 30% vulnerabilities on communication over a network among different peers. In order to investigate these fraudulent crimes, the investigation agencies (enforcement law) should make use of technology which is a crucial part.

All the network-based attacks are familiar threats that are launched by a device over a collection of devices and that single device will control the remaining devices in the network. These attacks are subcategories of cyber-crimes that include DOS (Denial of Service) attacks, Probe attacks, Worms, viruses and many other. Some of the cyber-attacks are hacking, banking frauds, and email spamming etc., are figured in Figure 1. Packet crafting is one such cyber-crime. It is a state-of-art mechanism to create a packet to carry out attacks according to various requirements and to exploit network vulnerabilities. Crafting is technically advanced and a complex type of vulnerability exploitation and is difficult to detect and diagnose. It is of active type mainly used to penetrate into a network’s structure. The digital forensic investigation is a branch of cyber forensics in which scientific methods and tools are used, that allows the prevention and analysis of digital evidence, that to be produced in a court of law.

In this paper, packet crafting crime is introduced along with its modules and later section presents diverse investigative tools related to packet crafting. These tools possess both positive (used by network administrators) and negative impacts (used by attackers).

2. PACKET CRAFTING
Packet crafting [3][4] is a procedure that allows network administrators to test the rules of firewall and observes all the entry points into a targeted system or network. This testing mainly aims at all types of components like Intrusion Detection System (IDS), firewall, router, TCP/IP stack of the network The behavior of network devices is scrutinized by creating packets in case of network traffic. Packets are generally made by using a packet generator or packet analyzer which allows for specific options and flags to be set on the created packets. In order to detect the properties of the network, crafting is used that imitated like an attack. To serve for that purpose, crafting breaks the protocols of both firewalls and intrusion detection software. Packet crafting is divided into four stages: Packet Assembly, Packet Editing, Packet Play and Packet Decoding presented in Figure 2.

Fig 1: Various Network-based attacks

Fig 2: Stages of Packet Crafting
2.1 Packet Assembly
It is the first step in packet crafting that an intruder makes the packet to collect the sensitive information from a targeted network. The packet should be designed in such a way that it should not be visible while passing through a network. Fig 3 demonstrates that the source address (10.0.0.5) is spoofed and transmits packet as it an ideal state.

2.2 Packet Editing
It defines the procedure of editing the content of an existing packet which is created or captured. The edited packets obtained relieve Packet Assembly process by manipulating packet’s overload. In this process, packets are tested before sending. All the packets are injected into a targeted network to retrieve the sensitive information to a maximum extent.

2.3 Packet Play/replay
For predictive analysis, It is procedure that sends generated packets to the targeted machine and collects the resultant packets in back. A series of captured packets/ pre-generated packets are sent using Packet Play or Packet Replay. Network attacks are the source for both Packet Assembly and Editing which is used to test a given attack scenario for the targeted network.

2.4 Packet Decoding
In this stage, the amount of data transferred during packet play at a point of time is interpreted. Later it observes the resultant packets generated from targeted source using a packet analyzer that decodes the relevant blueprints of captured packet. In response to that, a connection is set after packet played or transmitted. Then the intruder parses the information from those packets.

3. PACKET CRAFTING TOOLS
As shown in Figure 4. Hping, Nemesis, Ostinato, Cat Karat packet builder, Libcrafter, libtins, Scapy, Wirefloss, and Yersinia are some of the tools incorporated with Packet assembly process. Packet Editing involves modifying of recorded packets’ fields, checksums, and payloads in an easier manner for that Ostinato, Netdude is recommended.

All these modified packets are stored in pcap files for the purpose of replaying. All the stream lined and pcap formatted packets are transmitted through their original or user-defined rate using TCP-replay. Ostinato added support for pcap files in version 0.4. Packet replay can also be done by some packet analyzers. Various sniffing tools like Wireshark, TCP dump, dsniff, etc. are used for analyzing the packets [5].
Packet crafting which is one of such cyber-crimes happening during the communication of peers in a network. This paper also focuses on a brief expo of some packet crafting tools that are freely available over the Internet. Future work turns into the comparison various tools and mainly focuses on various algorithms to craft a packet under transmission.

4. CONCLUSIONS
Communication vulnerabilities are rising day-by-day in this cyber world. This paper gives a detailed description about Packet crafting which is one of such cyber-crimes happening during the communication of peers in a network. This paper also focuses on a brief expo of some packet crafting tools that are freely available over the Internet. Future work turns into the comparison various tools and mainly focuses on various algorithms to craft a packet under transmission.

5. REFERENCES