CYBER ATTACKS EXPLAINED: PACKET CRAFTING

Protect your FOSS-based IT infrastructure from packet crafting by learning more about it.

In the previous articles in this series, we explored common infrastructure vulnerability exploitation scenarios. This article takes a step forward to describe a technically advanced attack that could badly impact networks because it is tough to detect. Packet crafting is a commonly used and yet complex method to exploit vulnerabilities and, hence, it is important for network administrators to know more about it, and also to understand the various ways to protect their infrastructure against it. We will also look at how to protect FOSS-based systems from a packet crafting attack.

What is packet crafting?

Crafting, by definition, means to make or create something skillfully. As we know, all the vulnerability assessment tools used by network administrators to test the security of their networks are both a blessing and a curse. This is because the same set of tools can also be used by evil hackers to find vulnerabilities and then exploit those to their benefit. Packet crafting, too, is not an exception to this rule, and since

it is a technically advanced yet complex type of vulnerability exploitation, it is difficult to detect and diagnose.

Let's look at a TCP packet and its fields in detail, in order to understand a packet crafting attack better. Refer to Figure 1, which shows a basic Ethernet packet as well as the TCPIP packet frame that rides on top of it.

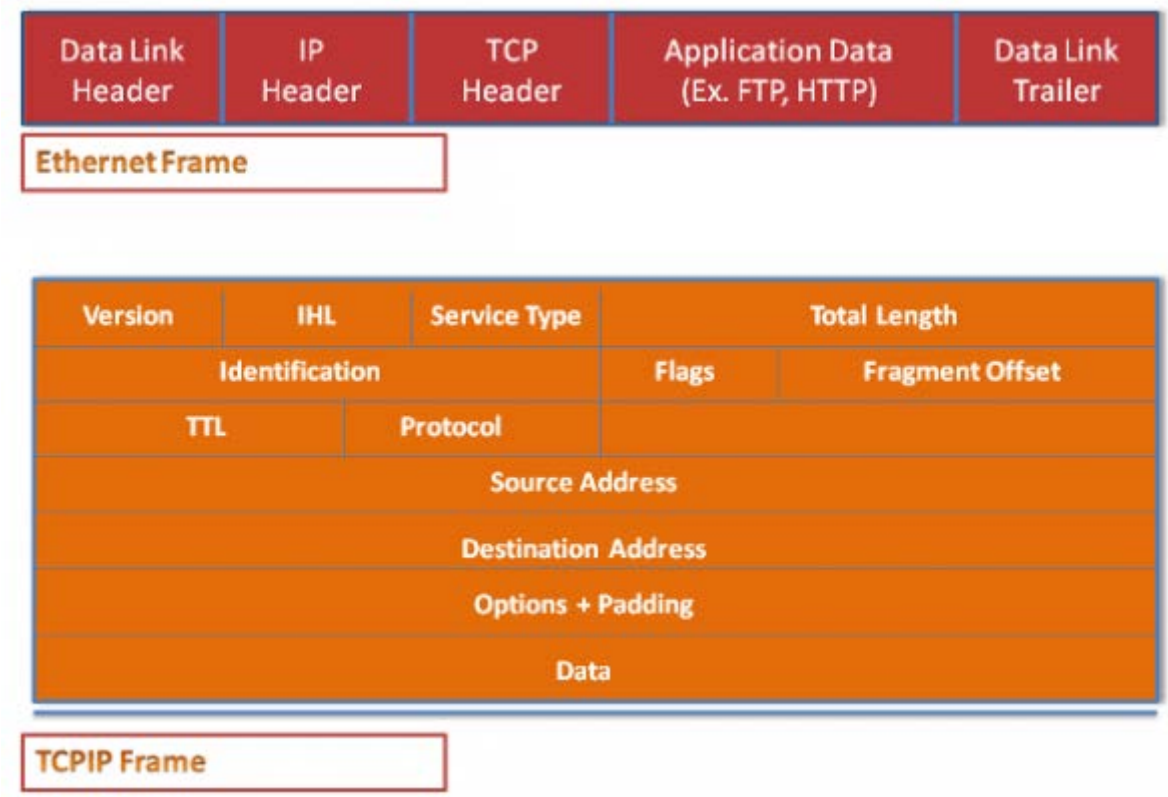

Figure 1: A basic Ethernet and TCPIP packet

The Ethernet frame contains multiple fields that typically take care of Layer-2 communication, whereas the TCP and IP packet chunks carry data fields for the upper layers. The TCP part of the packet ensures a successful transport, while the IP packet contains source and destination addresses and ports.

As mentioned in the previous articles of this series, we are aware that the TCP/IP communication comprises a three-way handshake (SYN, SYN-ACK, ACK), which sets up a communication channel between two network interface cards. The data flows between them through this channel, and it is terminated by using a FIN/FIN-ACK handshake.
Earlier articles also covered the fact that each of these packet fields can be modified by attackers for their benefit. The source and destination IP address or ports are very commonly attacked fields in the denial of service and spoofing

attacks, as well as in network penetrations. Here, it is important to understand that it’s not just these fields that could be modified, but in fact, each and every flag and field in a TCP frame and the underlying Ethernet frame can be modified or altered — all for the purpose of network penetration.

Please note that packet crafting and packet spoofing are often mistakenly assumed to be the same technique; however, they are very different from the impact standpoint. Spoofing is used by attackers to hide their identities and presence on the network. Spoofing is primarily used to gain network information such as open ports, running services, active hosts, etc., during which time the target host fails to trace the attacker.

On the other hand, packet crafting takes a step further by trying to test the presence, functionality or the accuracy of target network’s firewall rules, and intrusion detection systems. Packet crafting requires in-depth knowledge of TCP packets and how they work, and is more of a manually orchestrated attack than a programmatic one. This makes it a technically advanced way of trying to hack into networks.

Packet crafting in action

Packet crafting is a task that is methodically carried out to penetrate into a network’s infrastructure. Please refer to Figure 2, which shows the four distinct steps involved in the packet crafting attack.

Figure 2: The steps involved in packet crafting

Let’s understand each of these steps a bit more in detail.

Packet assembly

This is the first step in the crafting process, wherein an attacker decides which network needs to be cracked, tries to gather possible vulnerability information and creates or fabricates the packets to be sent. This packet is then checked for accuracy, especially to ensure that the attack is as “invisible” on the network as possible, to go undetected.

For example, the packet being created can have a spoofed source address and a dummy TCP sequence number. The assembly of a packet need not be done from scratch; a packet going over the wire can be captured and its contents can be modified to serve the hacking purpose.

Packet editing

In this step, usually a dry run on the assembled packet is tested and based on the results gathered, and the packet is tuned up or corrected before moving to the next step. In the editing phase, the focus is usually to gather the maximum amount of information by injecting the minimum number of packets into the network.

For example, to test how a firewall responds to malformed packets, a simple packet with a false source IP address and with ACK field bit set can be created. In ideal situations, the firewall should drop such a packet.

Packet playing

Once the correct packet or a stream of packets is created, “packet playing” sends it onto the network, and collects the resultant packets to perform further analysis and corelation. This is when an actual attack is performed. If the expected outcome is not achieved, hackers go back to the editing phase to change the attack scenario.

Packet analysing

In this process, the packet streams are gathered to decode the presented response by the target network. Attackers may use simple packet sniffing tools for this purpose, or can capture the packet streams in the form of a log file and analyse it. This step either provides evidence to the hackers that they were successful in penetration, or at least gives them enough inputs to tune up the attack, or change their methods.

Packet crafting techniques

As seen above, the whole idea behind packet crafting is to try to simulate an attack, thus learning the behaviour of various network devices in order to gain knowledge about the vulnerabilities. Crafting is typically used to invade into firewalls and intrusion detection devices, but can also be used to attack Web servers and other application gateways. Now let’s discuss a few common packet crafting techniques.

Ping fragmentation

In this type, instead of a standard ICMP ping packet, a malformed ping packet is created with more than 65,535 bytes, which is the maximum allowed in a packet. This results in the destination system responding with an echo reply, which also consumes a larger packet frame and thus eventually results in a denial of service attack.

One technique also sets an ACK flag in the packet, confusing the destination service, while in another type of attack, instead of a larger frame, a variable number of bytes are sent to overwhelm the system.

Packet flag manipulation

As we discussed before, there are multiple fields in the TCP datagram. One of the fields contains flags or bits, which could be set programmatically. For example, a SYN flag can be set and the packet can be sent over the wire to a destination to establish a valid TCP communication. This would be a healthy way of initiating a TCP handshake; however, it can be exploited by sending a RST or FIN packet, which can confuse the destination system.

Older firewalls are known to be susceptible to FIN attacks, because they cannot properly differentiate between a valid packet and a bogus FIN packet. In another variety, a malformed SYN-ACK packet or ACK packet can cause a similar effect.

Packet duplication

Here, attackers capture a series of packets and simply resend it over the network. This causes confusion at the destination system, which assumes that the previous session was not properly answered or terminated. A typical example of this attack is when a duplicate ACK or FIN packet is sent without modifying any other content of the packet frame. This method is commonly used in a denial of service attack.

Protocol manipulation

This is mainly used to test firewall vulnerabilities. Here the TCP and UDP flags are both set in a packet to confuse the firewall rule set. If the firewall is one of the latest, it can identify such a packet as a malformed one and will simply drop it.

However, for legacy firewalls, if there are multiple rules set to handle TCP and UDP packets, both rules get executed causing an erroneous effect, which can lead to the firewall shutting down. Another way is to not set the TCP or UDP flag at all — this tricks the switch devices managed by Layer 3.

Half open packets

In this method, attackers initiate a connection with a target host using a SYN packet. The target sends Syn-ACK; however, the hackers do not respond to it, and instead create a spoofed packet by changing the source IP and sending another SYN packet. This process continues, till the target host exhausts its resources, thus becoming a denial of service victim.

Protecting FOSS systems

As mentioned earlier, the packet crafting attack is a tough one to tackle. Despite this, there are ways to protect FOSS networks. The simple and correct method is to use packet crafting tools themselves, to test the infrastructure. The first step is to understand the network, and create security testing scenarios to test critical security components such as firewalls, routers, IDS systems, etc.

Tools such as Hping and TCPReplay could be used to fabricate packets and send them to gather statistics and logs. A packet sniffer and analyser such as Wireshark can be used for this purpose. Firewalls and IDS systems built on FOSS technology should be tested on Layer-2 through to Layer-7. Performing such tests at regular intervals and staying up-to-date with the intrusion detection vulnerability signatures is the appropriate way to be protected.

To protect FOSS Web servers, the latest Layer-7 content filtering firewall that is capable of performing a stateful packet inspection, and which is equipped to detect and shun a denial of service attack, should be implemented. Linux distros lack a strong built-in security module to fight against packet crafting attacks. Hence, a properly designed perimeter defence system should be deployed to protect the infrastructure.

Packet crafting is a good way to audit your network; however, it can be used by evil hackers to penetrate into a network, by exploiting vulnerabilities. Configure firewalls, switches and routers properly to prevent networks from crafting attacks. Packet crafting attacks typically can happen from outside the firm’s local area network, which demands a carefully designed perimeter defence security system for network infrastructure.

Source : http://www.opensourceforu.com/2012/05/cyber-attacks-explained-packet-crafting/