# Chapter 11

The toy tetragraph hash (tth) operates on letters instead of binary data. Given a message consisting of a sequence of letters, tth produces a hash value consisting of four letters.

First, tth divides the message into blocks of 16 letters, ignoring spaces, punctuation, and capitalization. If the message length is not divisible by 16, it is padded out with nulls. A four-number running total is maintained that starts out with the value (0, 0, 0, 0); this is input to the compression function for processing the first block. The compression function consists of two rounds.

Round 1 Get the next block of text and arrange it as a row-wise 4x4 block of text and convert it to numbers (A=0, B=1, etc.). For example, for the block ABCDEFGHIJKLMNOP, we have

|  |  |  |  |
| --- | --- | --- | --- |
| A | B | C | D |
| E | F | G | H |
| I | J | K | L |
| M | N | O | P |

|  |  |  |  |
| --- | --- | --- | --- |
| 0 | 1 | 2 | 3 |
| 4 | 5 | 6 | 7 |
| 8 | 9 | 10 | 11 |
| 12 | 13 | 14 | 15 |

Then, add each column mod 26 and add the result to the running total, mod 26. In this example, the running total is (24, 2, 6, 10).

Round 2 Using the matrix from round 1, rotate the first row left by 1, second row left by 2, third row left by 3, and reverse the order of the fourth row. In our example:

|  |  |  |  |
| --- | --- | --- | --- |
| B | C | D | A |
| G | H | E | F |
| L | I | J | K |
| P | O | N | M |

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | 2 | 3 | 0 |
| 6 | 7 | 4 | 5 |
| 11 | 8 | 9 | 10 |
| 15 | 14 | 13 | 12 |

Now, add each column mod 26 and add the result to the running total. The new running total is (5, 7, 9, 11). This running total is now the input into the first round of the compression function for the next block of text. After the final block is processed, convert the final running total to letters. For example, if the message is ABCDEFGHIJKLMNOP, then the hash is FHJL.

1. Draw figures comparable to Figures 11.9 and 11.10 to depict the overall tth logic and the compression function logic.
2. Calculate the hash function for the 48-letter message “I leave twenty million dollars to my friendly

cousin Bill.”

1. To demonstrate the weakness of tth, find a 48-letter block that produces the same hash as that

just derived. Hint: Use lots of A’s.

# Chapter 6

* 1. What are three broad mechanisms that malware can use to propagate?

•Infection of existing content by viruses that is subsequently spread to other systems

•Exploit of software vulnerabilities by worms or driveby-downloads to allow the malware to replicate

•Social engineering attacks that convince users to bypass security mechanisms to install Trojans or to respond to phishing attacks

* 1. What are four broad categories of payloads that malware may carry?

•Corruption of system or data files

•Theft of service/make the system a zombie agent of attack as part of a botnet

•Theft of information from the system/keylogging

•Stealthing/hiding its presence on the system

* 1. What characteristics of an advanced persistent threat give it that name?

**Advanced**

* Used by the attackers of a wide variety of intrusion technologies and malware including the development of custom malware if required

**Persistent**

* A variety of attacks may be progressively applied until the target is compromised

**Threats**

* Threats to the selected targets as a result of the organized, capable, and well-funded attackers intent to compromise the specifically chosen targets
  1. What are typical phases of operation of a virus or worm?
* Dormant phase(virus is idle not all viruses have this stage)
* Triggering phase(virus is activated)
* Propagation phase(Propagation mechanism)
* Execution phase(function is performed)
  1. What mechanisms can a virus use to conceal itself?
* Encryption via random encryption key. Stealth hides itself from detection in the system. Polymorphism changes with each infection to avoid detecting by a signature. Metamorphism rewrites itself entirely at each iteration to increase the complexity of detection.
  1. What is the difference between machine executable and macro viruses?
* Machine executable viruses affect all other executable files on the system, if the infected program executes. Macro viruses affect only the documents on the system, if they have macro or scripting code.
  1. What means can a worm use to access remote systems to propagate?
* Email or instant messengers to transmit a copy of itself. File sharing on removable media like a USB drive. Remote execution explicitly or through a program error in a network service. Remote file access or transfer capability to copy to another system. Remote login capability acts as a user and uses commands to duplicate itself from one system to another duplicate system
  1. What is a “drive-by-download” and how does it differ from a worm?
* A drive-by-download uses code that exploits browser bugs to download and fit malware on the user's system without their knowledge. It does not spread vigorously like a worm, but rather waits for a user to view the malicious web page.
  1. How does a Trojan enable malware to propagate? How common are Trojans on computer systems? Or on mobile platforms?
* A Trojan is a program containing a hidden code, which executes to perform its attack. Sometimes the Trojan is inserted into a game or utility program and made available in an application store. They are very common on computer systems and often carry spyware. Trojans on mobile platforms generally come from app market places.
  1. What is a “logic bomb”?
* It is a code inserted in malware that is placed to "explode" when certain actions occur. Triggers could include: presence or absence of devices/files on system, a date or time, a software with an appropriate version/configuration, or an application being executed.
  1. What is the difference between a backdoor, a bot, a keylogger, spyware, and a rootkit? Can they all be present in the same malware?
* A backdoor is a secret access point in a system. A bot abuses resources of the infected system. A keylogger records every keystroke. Spyware observes information on the system such as browsing history and content. A rootkit is a collection of programs implemented on the system to sustain secret access with admin rights. And yes, they can all be present in the same malware.
  1. What is the difference between a “phishing” attack and a “spear-phishing” attack, particularly in terms of who the target may be?
* The goal of phishing attacks is to send a spoofed email that looks as if it is from an authentic organization to a large number of people. Spear-phishing targets a specific victim, and messages are modified to specifically address that victim.
  1. List some the different levels in a system that a rootkit may use.
* In user mode, it can cut off API calls and change returned results. In kernel mode, it can cut off kernel API calls and hide its existence in kernel tables. In virtual machine based mode, it can cut off and change state and events taking place in the virtualized system. In external mode, it can access the hardware directly, such as BIOS and system management mode.
  1. Describe some malware countermeasure elements
* Detect the positions of the malware. Identify the specific malware that has infected the system. Remove all elements of malware from every infected system so it cannot propagate further.
  1. List three places malware mitigation mechanisms may be located.
* On the infected system, where some host-based "anti-virus" program is running, monitoring data imported into the system, and the execution and behavior of programs running on the system; as part of the perimeter security mechanisms used in an organization's firewall and intrusion detection systems, or it may use distributed mechanisms over a huge amount of networks and organizations to get the main scale perspective of the movement of malware.
  1. Briefly describe the four generations of anti-virus software.
* First generation needs "simple scanners" to determine the malware. Second generation needs "Heuristic scanners" to search for possible malware using heuristic rules or needs an "integrity checking" to determine changed files. Third generation needs "activity traps" in an infected program to determine malware by its measures rather than its structure. Fourth generation needs "full-featured protection" using a collection of anti-virus techniques packages in conjunction, with activity trap components and scanning.

# Chapter 7

* 1. Define a denial-of-service (DoS) attack.
* An action that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources such as central processing units (CPU), memory, bandwidth, and disk space
  1. What types of resources are targeted by such DoS attacks?
* Memory
* Bandwidth
* CPU
* Disk space
  1. What is the goal of a flooding attack?
* Load the network capacity on some link to a server, or overload the capability of the server to handle and respond to traffic
  1. What types of packets are commonly used for flooding attacks?
* ICMP Packets
* TCP SYN
* UDP
  1. Why do many DoS attacks use packets with spoofed source addresses?
* **Anonymity: to hide his identity**
* **Avoiding Detection from network security solution like Firewalls,IPS and IDS**
* **Reflection and Amplification attacks**
  1. What is “backscatter traffic?” Which types of DoS attacks can it provide information on? Which types of attacks does it not provide any information on?
  + Backscatter traffic is a side effect of spoofed DoS/DDoS attacks. The victim responds to the spoofed packets as it normally would, and the traffic generated by these responses is called the backscatter traffic. Backscatter traffic can provide information on certain types of DoS attacks, especially those involving reflection and amplification techniques, Backscatter traffic may not provide information on certain types of DoS attacks, especially those that involve direct flooding without relying on reflection or amplification
  1. Define a distributed denial-of-service (DDoS) attack.
* The attacker uses a botnet to significantly increase the volume of traffic flooding the target system
  1. What architecture does a DDoS attack typically use?

Typically uses a control hierarchy approach, where the attacker controls the small number of handler systems, and the handles control the large number of agent systems

* 1. Define a reflection attack.

The **reflection attack** is a direct implementation of this type of attack. The attacker sends packets to a known service on the intermediary with a spoofed source address

of the actual target system. When the intermediary responds, the response is sent to the target. Effectively this reflects the attack off the intermediary, which is termed the reflector

* 1. Define an amplification attack.

Amplification attacks generate a high volume of packets to flood the target website without alerting the intermediary, by returning a large reply to a small request. The attacker exploits vulnerabilities in DNS servers to turn initially small queries into much larger payloads. It is a type of reflection attack which manipulates publically-accessible DNS

* 1. What is the primary defense against many DoS attacks, and where is it implemented?
* Block spoofed source addresses
  + - On routers as close to source as possible
  + Filters may be used to ensure path back to the claimed source address is the one being used by the current packet
    - Filters must be applied to traffic before it leaves the ISP’s network or at the point of entry to their network
  1. What defenses are possible against nonspoofed flooding attacks? Can such attacks be entirely prevented?
* replicated distributed servers when overload on the network is predicted
* Rate limits.
* IPS and Firewalls

It may be challenging to prevent such attacks but when using good security solutions it may be entirely prevented

* 1. What defenses are possible against TCP SYN spoofing attacks?
* Firewall to filter packets
* **SYN Cookies**
  1. What defenses are possible against a DNS amplification attack? Where must these be implemented? Which are unique to this form of attack?
* prevent the use of spoofed source addresses
* Appropriate configuration of DNS servers, in particular limiting recursive responses to internal client systems
* **DNS Rate Limiting**

**These defenses should be implemented at various level on the network specially on the DNS servers**

* 1. What defenses are possible to prevent an organization’s systems being used as intermediaries in a broadcast amplification attack?
* The best defense against broadcast amplification attacks is to block the use of IP-directed broadcasts. This can be done either by the ISP or by any organization whose systems could be used as an intermediary
  1. To what do the terms slashdotted and flash crowd refer to? What is the relation between these instances of legitimate network overload and the consequences of a DoS attack?
* They refer to huge volumes of legitimate traffic on the system that will lead to devastation of the system's network connection. This happens sometimes as a result of high popularity regarding a particular web site. these events are not malicious in nature, they share similarities with the consequences of a Denial of Service (DoS) attack, specifically in terms of overwhelming network resources and causing service disruptions.
  1. What steps should be taken when a DoS attack is detected?
* Good Incident Response Plan
* Antispoofing, directed broadcast, and rate limiting filters should have been implemented
* Ideally have network monitors and IDS to detect and notify abnormal traffic patterns
  1. What measures are needed to trace the source of various types of packets used in a DoS attack? Are some types of packets easier to trace back to their source than others?
* Have ISP trace packet flow back to source. Difficult and time consuming to trace spoofed addresses back to the source.