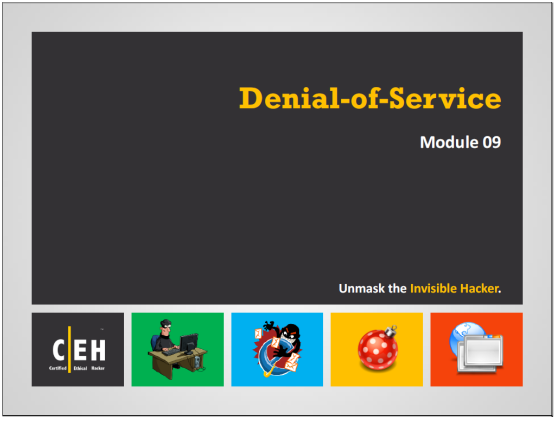
Denial-of-Service

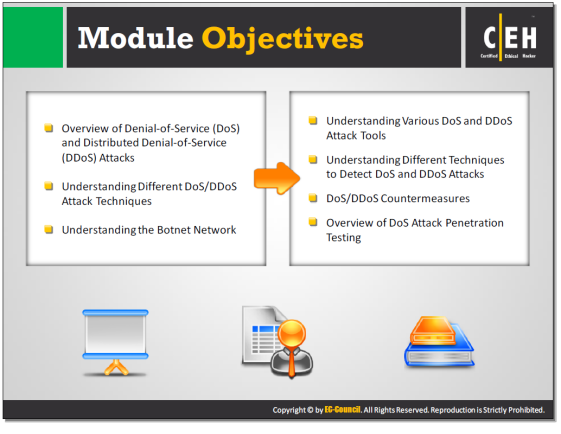
Module 09



Ethical Hacking and Countermeasures v9

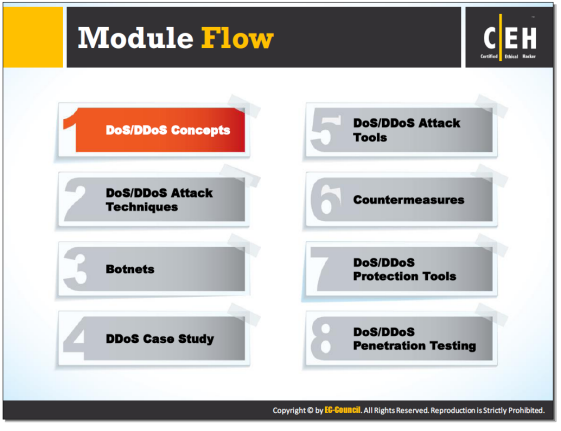
Module 09: Denial-of-Service

Exam 312-50

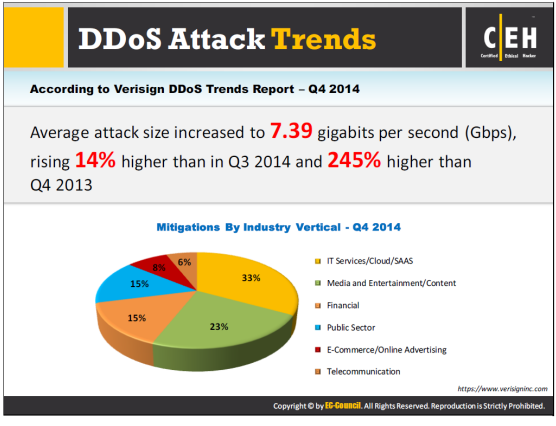


Denial of Service (DoS) and **Distributed Denial of Service** (DDoS) attacks have become a major threat to present computer networks. These attacks attempt to make a machine or network resource unavailable to its authorized users. Usually DoS/DDoS attacks exploit vulnerabilities in implementation of TCP/IP model protocol or bugs in a specific operating system.

This module starts with an overview of DoS and DDoS attacks. It provides an insight into different DoS/DDoS attack techniques. Later, it discusses about botnet network, DoS/DDoS attack tools, techniques to detect DoS/DDoS attacks, and DoS/DDoS countermeasures. The module ends with an overview of pen-testing steps an ethical hacker should follow to perform a security assessment of the target.



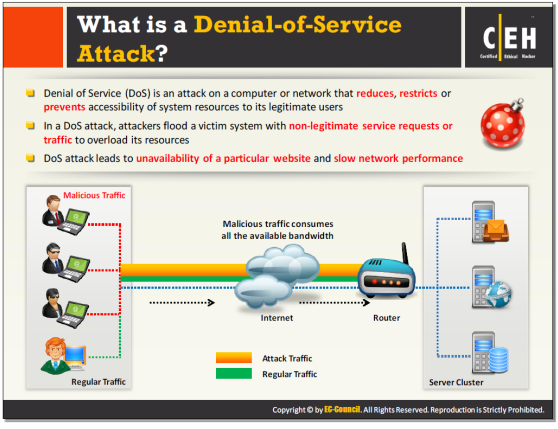
For better understanding of DoS/DDoS attacks, one must be familiar with DoS/DDoS concepts beforehand. This section deals with what a DOS Attack is, what a DDoS Attack is, and how the DDoS attacks work.



According to the observations and insights derived from customers of **VeriSign DDoS Protection Services** and the security research of **VeriSign iDefense Security Intelligence Services** (during the period October 1–December 31, 2014), the average attack size increased to 7.39 gigabits per second (Gbps), rising 14 percent higher than in third quarter of 2014 and 245 percent higher than the fourth quarter of 2013. The most frequently targeted industries during the fourth quarter were IT Services/Cloud/SaaS, representing one-third of all mitigation activity and peaking at just over 60 Gbps.

DDoS attacks are a global threat and not limited to any specific industry vertical. In the fourth quarter, IT Services/Cloud/SaaS customers experienced the largest volume of attacks, representing one-third of all attacks and peaking in size at just over 60 Gbps, followed by Media and Entertainment/Content customers with 23%, and financial customers with 15%.

Source: *https://www.verisigninc.com*



In a denial-of-service (DoS) attack, an attacker overloads a system's resources, bringing the system down, or at least significantly slowing system performance. The goal of a DoS attack is not to gain unauthorized access to a system or to corrupt data; it is to keep away legitimate users from using the system.

The following are examples of types of DoS attacks:

- Flooding the victim with more traffic than can be handled
- Flooding a service (like IRC) with more events than it can handle
- Crashing a TCP/IP stack by sending corrupt packets
- Crashing a service by interacting with it in an unexpected way
- Hanging a system by causing it to go into an infinite loop

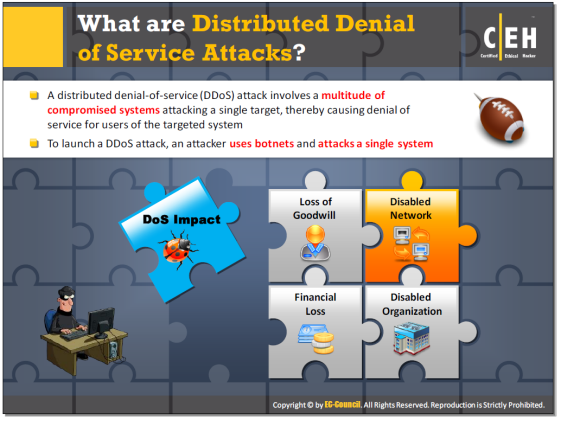
DoS attacks come in a variety of forms and target a variety of services. The attacks may cause the following:

- Consumption of scarce and nonrenewable resources
- Consumption of bandwidth, disk space, CPU time, or data structures
- Actual physical destruction or alteration of network components
- Destruction of programming and files in a computer system

In general, DoS attacks target network bandwidth or connectivity. Bandwidth attacks overflow the network with a high volume of traffic using existing network resources, thus depriving legitimate users of these resources. Connectivity attacks overflow a computer with a large amount of connection requests, consuming all available operating system resources so that the computer cannot process legitimate users' requests.

Imagine a pizza delivery company, which does much of its business over the phone. If an attacker wanted to disrupt this business, he could figure out a way to tie up the company's phone lines, making it impossible for the company to do business. That is how a denial-of-service attack works—the attacker uses up all the ways to connect to the system, making legitimate business impossible.

DoS attacks are a kind of security break that does not generally result in the theft of information. However, these attacks can harm the target in terms of time and resources. On the other hand, failure might mean the loss of a services such as email. In a worst-case scenario, a DoS attack can mean the accidental destruction of the files and programs of millions of people who happen to be surfing the Web at the time of the attack.



A distributed denial-of-service (DDoS) attack is a large-scale, coordinated attack on the availability of services on a victim's system or network resources, launched indirectly through many compromised computers on the Internet.

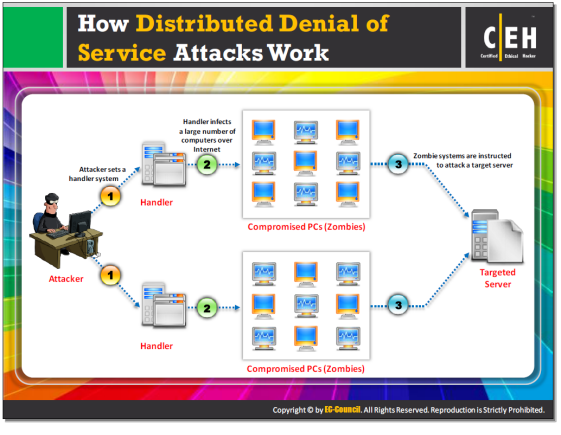
As defined by the World Wide Web Security FAQ: "A distributed denial-of-service (DDoS) attack uses many computers to launch a coordinated DoS attack against one or more targets. Using client/server technology, the perpetrator is able to multiply the effectiveness of the denial of service significantly by harnessing the resources of multiple unwitting accomplice computers, which serve as attack platforms." The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the legitimate users.

The services under attack are those of the "**primary victim**," while the compromised systems used to launch the attack are the "secondary victims." The use of secondary victims in performing a DDoS attack provides the attacker with the ability to wage a larger and a more disruptive attack, while making it more difficult to track down the original attacker.

The main objective of any DDoS attacker is to first gain administrative access on as many systems as possible. Generally, attackers use customized attack script to identify potentially vulnerable systems. Once the attacker gains access to the target systems, he or she will upload DDoS software and run it on these systems, but not until the time chosen to launch the attack.

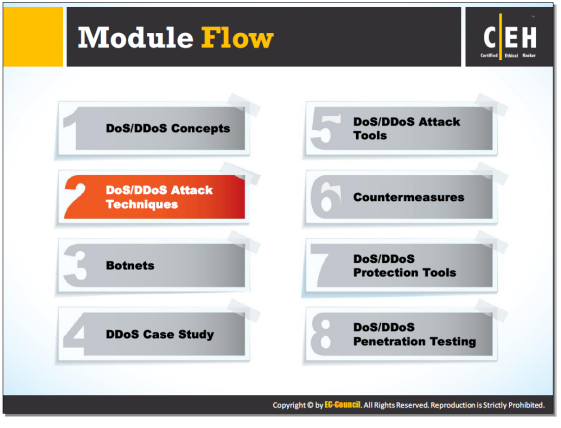
Distributed denial-of-service attacks have become popular because of the easy accessibility of exploit plans and the negligible amount of brainwork required while executing them. These attacks can be very dangerous because they can quickly consume the largest hosts on the Internet, rendering them useless. The impact of DDoS includes loss of goodwill, disabled network, financial loss, and disabled organizations.

Source: *www.searchsecurity.com*

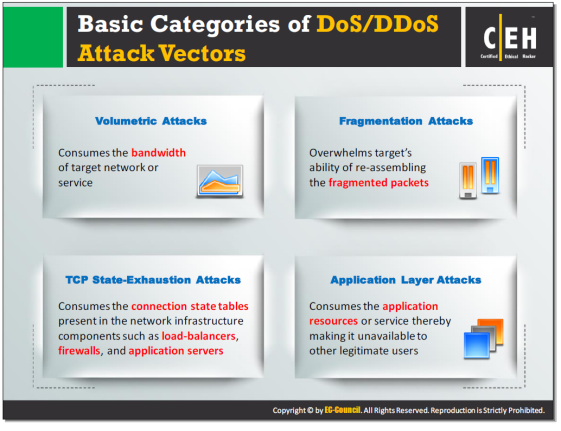


In a DDoS attack, many applications pound the target browser or network with fake exterior requests that make the system, network, browser, or site slow, useless, and disabled or unavailable.

The attacker initiates the DDoS attack by sending a command to the zombie agents. These zombie agents send a connection request to a large number of reflector systems with the spoofed IP address of the victim. The reflector systems see these requests as coming from the victim machine instead of the zombie agents due to spoofing of source IP address. Hence, they send the requested information (response to connection request) to the victim. The victim machine is flooded with unsolicited responses from several reflector computers at once. This either may reduce the performance or may cause the victim machine to shut down completely.



Attackers implement various techniques to launch DoS/DDoS attacks on target computers or networks. This section deals with the basic categories of DoS/DDoS attack vectors and various DoS attack techniques that include bandwidth attacks and service request floods, SYN flooding attack, ICMP flood attack, Peer-to-Peer attacks, application-level flood attacks, permanent Denial-of-Service attack, and Distributed reflection Denial of Service (DrDoS).



DDoS attacks mainly aim at the exhaustion of network, application or service resources, thereby restricting the legitimate users from accessing their system or network resources. In general, the following are the categories of DoS/DDoS attack vectors:

- **Volumetric Attacks**

  These attacks exhaust the bandwidth either within the target network/service, or between the target network/service and the rest of the Internet, and result in traffic blockage. Magnitude is measured in bits-per-second.

- **Fragmentation Attacks**

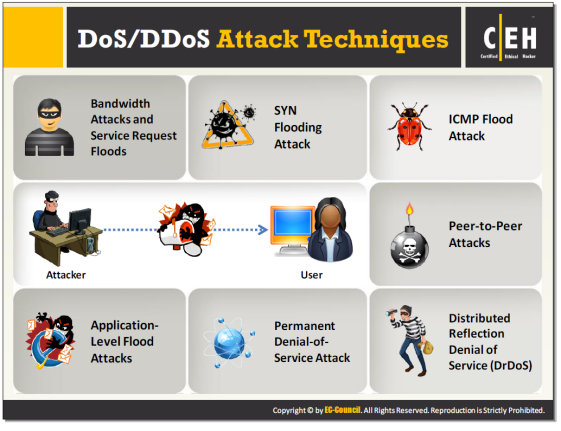
  These attacks destroy a victim's ability to re-assemble the fragmented packets by flood with TCP or UDP fragments to the victim, resulting in reduced performance.

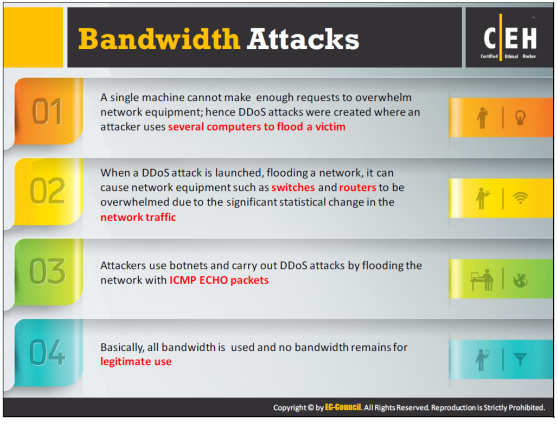
- **TCP State-Exhaustion Attacks**

  These attacks consume the connection state tables present in the network infrastructure devices such as load-balancers, firewalls, and application servers. These attacks can even take over state of millions of connections maintained by high capacity devices. Magnitude is measured in packets-per-second.

- **Application Layer Attacks**

  These attacks destroy a specific aspect of an application or service and are effective with one or few attacking machines producing a low traffic rate (very hard to detect and mitigate). Magnitude of the attack is measured in requests-per-second.

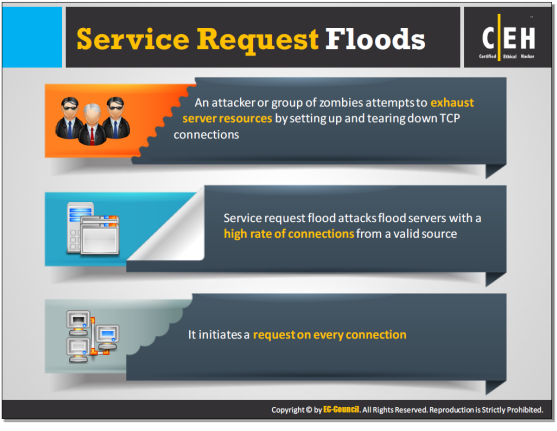




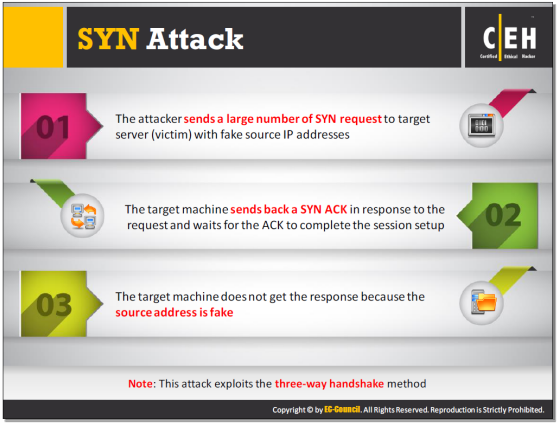
Generation of a large number of packets can cause the consumption of all the bandwidth on the network. Typically, these packets are ICMP echo packets. A single machine cannot make enough requests to overwhelm network equipment. Hence, in DDoS attacks, the attacker uses several computers to flood a victim. In this case, the attacker can control all the machines and instruct them to direct traffic to the target system. DDoS attacks flood a network overwhelming network equipment such as switches and routers with the significant statistical change in the network traffic. Attackers use the processing power of a large number of geographically distributed machines to generate huge traffic directed to the victim, which makes it a distributed-denial-of-service (DDoS) attack.

There are two types of bandwidth depletion attacks. A flood attack involves zombies sending large volumes of traffic to victim systems in order to clog these systems' bandwidth. An amplification attack engages the attacker or zombies to transfer messages to a broadcast IP address. This method amplifies malicious traffic that consumes victim systems' bandwidth.

Attackers use botnets and carry out DDoS attacks by flooding the network with ICMP ECHO packets. All bandwidth is used, and no bandwidth remains for legitimate use.



Service request floods work on the connections per second principle. In this method or technique of a DoS attack, the servers are flooded with a huge number of service requests (for setting up a connection), such as HTTP requests, TCP three-way handshake requests, and VPN setup requests, from a valid source. In these attacks, an attacker or group of zombies attempts to exhaust server resources by setting up and tearing down TCP connections. This probably initiates a request on each connection; for example, an attacker may use his or her zombie army to fetch the home page from a target web server repeatedly. The resulting load on the server makes it sluggish.



In a SYN attack, the attacker sends a large number of SYN request to target server (victim) with fake source IP addresses. The attack creates incomplete TCP connections that use up network resources. Normally, when a client wants to begin a TCP connection to a server, the client and the server exchange a series of messages, as follows:

- A TCP SYN (synchronize packet) request is sent to a server.
- The server sends back a SYN/ACK (acknowledgement) in response to the request.
- The client sends a response ACK to the server to complete the session setup.

The above method is the three-way handshake.

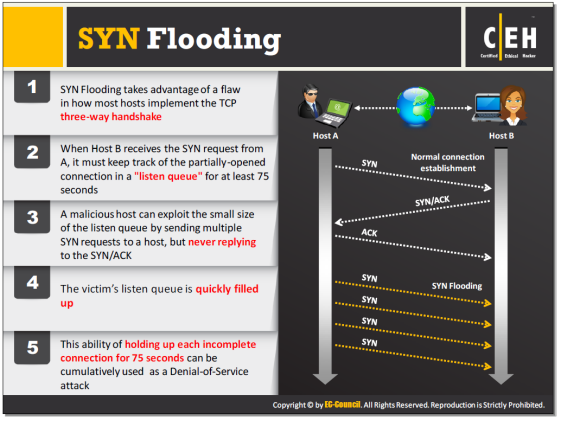
In a SYN attack, the attacker exploits the three-way handshake method. First, the attacker sends a fake TCP SYN request to the target server and when the server sends back a SYN/ACK in response to the client (attacker) request, the client never sends an ACK response. This leaves the server waiting to complete the connection.

Countermeasures

Proper packet filtering is a viable solution. An administrator can also modify the TCP/IP stack. Tuning the TCP/IP stack will help reduce the impact of SYN attacks while allowing legitimate client traffic through.

Some SYN attacks do not attempt to upset servers, but instead try to consume all the bandwidth of the Internet connection. Two tools to counter this attack are SYN cookies and SynAttackProtect.

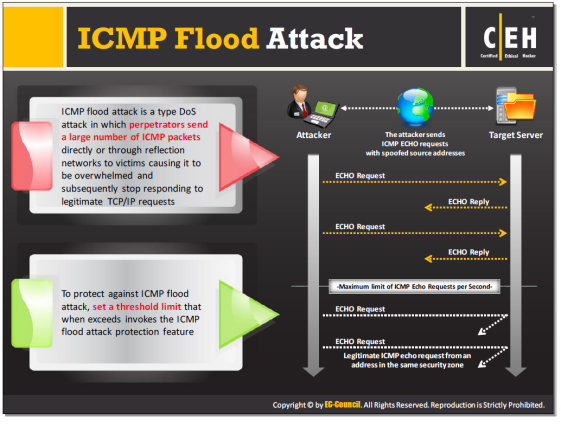
To guard against an attacker trying to consume the bandwidth of an Internet connection, an administrator can implement some additional safety measures. For example, decreasing the time-out period for keeping a pending connection in the SYN RECEIVED state in the queue can block such an attack. Normally, if a client sends no response ACK, a server will retransmit the first ACK packet. Decreasing the time of the first packet retransmission, decreasing the number of packet retransmissions, or turning off packet retransmissions entirely can erase this vulnerability.



SYN flooding takes advantage of a flaw in how most hosts implement the TCP three-way handshake. This attack occurs when the intruder sends unlimited SYN packets (requests) to the host system. The process of transmitting such packets is faster than the system can handle.

Normally, the connection establishes with the TCP three-way handshake. The host keeps track of the partially open connections, while waiting for response ACK packets in a listening queue. A malicious host can exploit the host managing many partial connections by sending many SYN requests to the host at once.

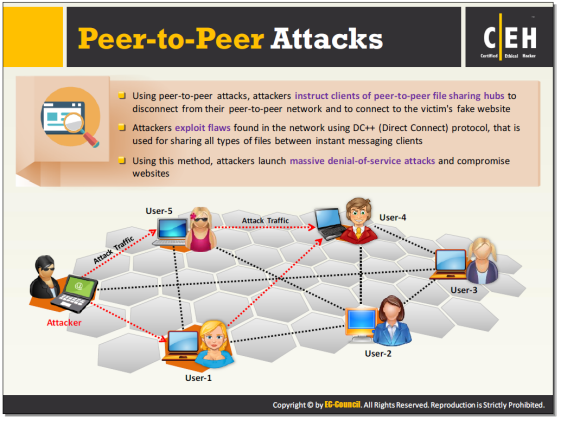
When the queue is full, the system cannot open new connections until it drops some entries from the connection queue (due to handshake timeout). This attack uses fake IP addresses, so it is difficult to trace the source. An attacker can fill table of connections even without spoofing the source IP address.



Network administrators use ICMP primarily for IP operations, troubleshooting, and error messaging of undeliverable packets. ICMP Flood Attack is a type DoS attack in which perpetrators send a large number of ICMP packets—directly or through reflection networks—to victims, causing it to be overwhelmed and subsequently stop responding to legitimate TCP/IP requests.

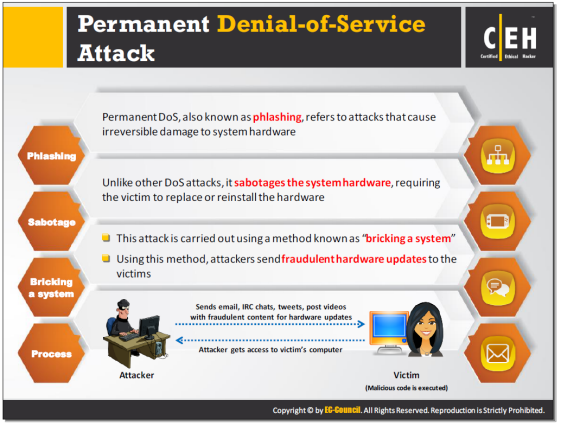
Similarly, a DDoS ICMP flood attack occurs when zombies send large volumes of ICMP echo request packets to a victim system. These packets signal the victim's system to reply, and the combination of traffic saturates the bandwidth of the victim's network connection. In the ICMP flood attack, attackers spoof the source IP address.

To protect against ICMP flood attack, set a threshold limit that when exceeds invokes the ICMP flood attack protection feature. When the ICMP threshold exceeds (by default the threshold value is 1000 packets/second), the router rejects further ICMP echo requests from all addresses in the same security zone for the remainder of the current second and the next second as well.



A peer-to-peer attack is one form of DDoS attack. In this kind of attack, the attacker exploits a number of bugs in peer-to-peer servers to initiate a DDoS attack. Attackers exploit flaws found in the network that uses DC++ (Direct Connect) protocol, which allows the exchange of files between instant messaging clients. This kind of attack does not use botnets for the attack. Unlike a botnet-based attack, a peer-to-peer attack eliminates the need of attackers to communicate with the clients it subverts. Here the attacker instructs clients of large peer-to-peer file sharing hubs to disconnect from their peer-to-peer network and instead, to connect to the victim's website. With this, several thousand computers may aggressively try to connect to a target website, which causes a drop in the performance of the target website. It is easy to identify peer-to-peer attacks based on signatures. Using this method, attackers launch massive denial-of-service attacks and compromise websites.

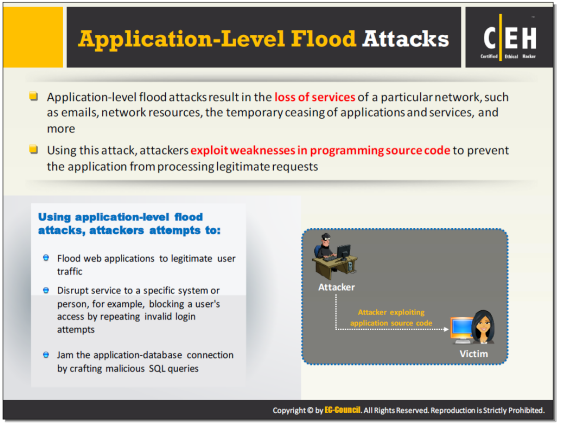
You can minimize the peer-to-peer DDoS attacks by specifying ports for peer-to-peer communication. For example, specifying port 80 not to allow peer-to-peer communication minimizes the possibility of attacks on websites.



Permanent Denial-of-Service (PDoS) attacks, also known as phlashing, purely target hardware. The PDoS is an attack that damages the system and makes its hardware unusable for its original purpose until the user replaces or reinstalls it. Unlike the DDoS attack, a PDoS attack exploits security flaws in a device, thereby allowing the remote administration on the management interfaces of the victim's hardware, such as printers, routers, or other networking devices.

This attack is quicker and is more destructive than the traditional DoS attack. It works with a limited number of resources, unlike a DDoS attack, in which attackers enforce a set of Zombies onto a target.

Attackers perform this attack using a method known as "**bricking a system**." In this method, the attacker sends email, IRC chats, tweets, and post videos with fraudulent content for hardware updates to the victim by modifying and corrupting the updates with vulnerabilities or defective firmware. When the victim clicks on the links or pop-up windows referring to the fraudulent hardware updates, the victim's system installs them. Thus, the attacker gets complete control over the victim's system.

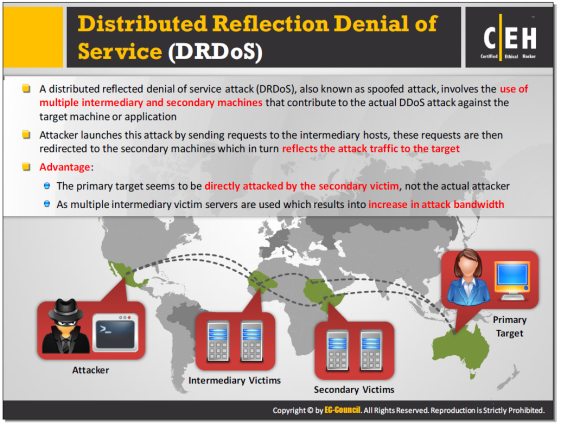


Application-level flood attacks result in the loss of the services of a particular network, such as emails, network resources, the temporary ceasing of applications and services, etc. Using this attack, attackers exploit weaknesses in programming source code to prevent the application from processing legitimate requests.

Several kinds of DoS attacks rely on software-related exploits such as buffer overflows. A buffer overflow attack is a type of attack that sends excessive data to an application that either brings down the application or forces the data sent to the application to run on the host system. The attack crashes a vulnerable system remotely by sending excessive traffic to an application.

Sometimes, attackers are also able to execute arbitrary code on the remote system via buffer overflow vulnerability. Sending too much data to the application overwrites the data that controls the program, and runs the hacker's code instead.

Application-level flood attacks can result in substantial loss of money, service, and reputation for organizations. These attacks occur after the establishment of a connection. Because the connection is established and the traffic entering the target appears to be legitimate, it is difficult to detect these attacks. However, if the user identifies the attack, he or she can stop it and trace back to a specific source more easily than other types of DDoS attacks.



A distributed reflected denial of service attack (DRDoS), also known as a "**spoofed**" attack, involves the use of multiple intermediary and secondary machines that contribute to the actual DDoS attack against the target machine or application. The DrDoS attack exploits the TCP three-way handshake vulnerability.

This attack involves attacker machine, intermediary victims (zombies), secondary victims (reflectors), and the target machine. Attacker launches this attack by sending requests to the intermediary hosts, which in turn reflect the attack traffic to the target.

The process involved in DrDoS attack:

First, the attacker commands the intermediary victims (zombies) to send a stream of packets (TCP SYN) with the primary target's IP address as the source IP address to other non-compromised machines (secondary victims or reflectors) to exhort them to establish connection with the primary target. As a result, the reflectors sends a huge volume of traffic (SYN/ACK) to the primary target to establish a new connection with it, as they believe it was the host that asked for it. The primary target discards the SYN/ACK packets received from the reflectors, as they did not send the actual SYN packet.

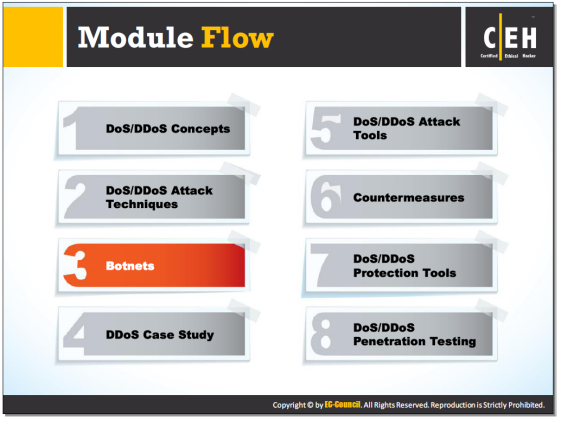
The reflectors keep waiting for the acknowledgement (ACK) response from the primary target. Assuming that the packet lost its path, these bunches of reflector machines resend SYN/ACK packets to the primary target in an attempt to establish the connection, until time-out occurs. This way, a heavy volume of traffic is flooded onto the target machine with the available

reflector machines. The combined bandwidth of these reflector machines overwhelms the target machine.

DrDoS attack is an intelligent attack, as it is very difficult or even impossible to trace the attacker. The secondary victim (reflector) seems to directly attack the primary target, but not the actual attacker. This attack is more effective than a typical DDoS attack as multiple intermediary and secondary victims generate huge attack bandwidth.

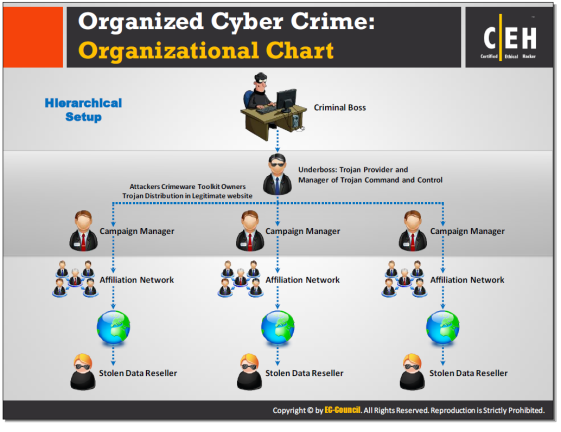
Countermeasures

- Turn off the Character Generator Protocol (CHARGEN) service to stop this attack method.
- Download the latest updates and patches for servers.



The term "**bot**" is a contraction of "**robot**." Attackers use bots to infect a large number of computers that form a network, or "botnet," allowing them to launch DDoS attacks, generate spam, spread viruses, and commit other types of crime.

This section deals with organized cyber-crime syndicates: organizational charts, botnet and their propagation techniques, botnet ecosystems, scanning methods for finding vulnerable machines, and propagation of malicious code.



Organized Crime Syndicates

Cyber criminals used to work independently, but now they tend to operate in organized groups. They are increasingly associated with organized crime syndicates to take advantage of their sophisticated techniques to engage in illegal activity, usually for monetary benefit. There are organized groups of cyber criminals who work in a hierarchical setup with a predefined revenue-sharing model—a kind of major corporation that offers criminal services. Organized groups create and rent botnets and offer various services, from writing malware, to hacking bank accounts, to creating massive denial-of-service attacks against any target for a price.

Example:

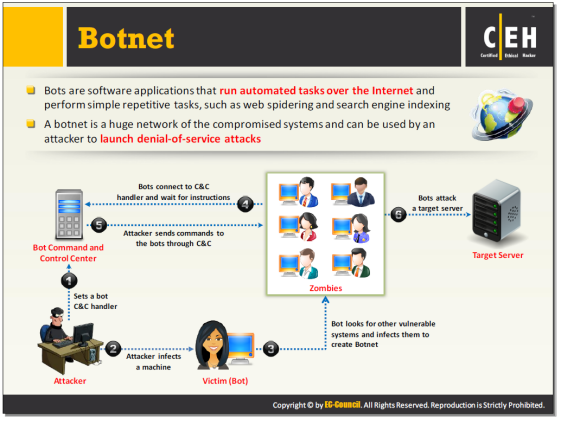
An organized crime syndicate might carry out a Distributed Denial of Service (DDoS) attack against a bank to divert the bank's security team while they clean out bank accounts with stolen account credentials.

According to **Prolexic's Q1 2014 global DDoS attack report**, total attacks in Q1 2014 increased 18 percent compared to Q1 2013.

The growing involvement of organized criminal syndicates in politically motivated cyber warfare and hacktivism is a matter of concern for national security agencies.

Cybercrime features a complicated range of players. Cyber criminals are paid according to the task they perform or the position they hold.

The head of the cyber-crime organization (i.e., the boss) acts as a business entrepreneur. The boss does not commit any crimes directly. Just below the boss is the "**underboss**," who sets up a Command and Control Server and Crimeware Toolkit Database, and manages implementation of attacks and providing the Trojans. Beneath the underboss are various "**campaign managers**" with their own affiliation networks for implementing attacks and stealing data. Finally, the resellers sell the stolen data.



Bots are software applications that run automated tasks over the Internet. Attackers use bots for benign data collection, or data mining, such as "**Web spidering**," as well as to coordinate DoS attacks. The main purpose of a bot is to collect data. There are different types of bots, such as Internet bots, IRC bots, and chatter bots. Some IRC bots are Eggdrop, Winbot, Supybot, Infobot, and EnergyMech.

A botnet (from "**roBOT NETwork**") is thus a group of computers "**infected**" by bots; however, botnets can be used for both positive and negative purposes. As a hacking tool, a botnet can be composed of a huge network of compromised systems. A relatively small botnet of only 1,000 bots has a combined bandwidth that is larger than the Internet connection of most corporate systems.

The advent of botnets led to an enormous increase in cyber-crime. Botnets form the core of the cyber-criminal activity center that links and unites various parts of the cyber-criminal world. Cyber-criminal service suppliers are a part of cybercrime network. They offer services such as malicious code development, bulletproof hosting, creation of browser exploits, and encryption and packing.

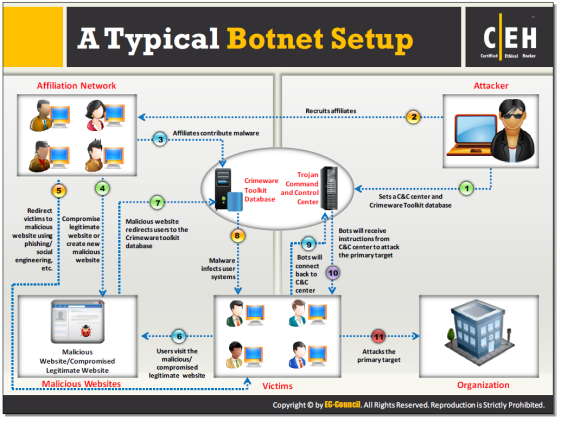
Malicious code is the main tool used by criminal gangs to commit cyber-crimes. Botnet owners order both bots and other malicious programs such as Trojans, viruses, worms, keyloggers, and specially crafted applications to attack remote computers via networks. Developers offer malware services on public sites or closed Internet resources.

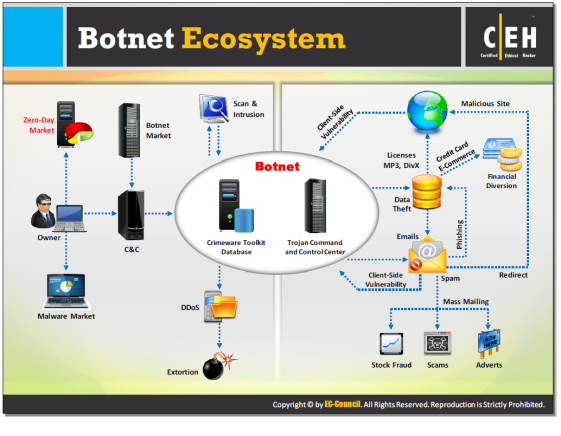
Botnets are agents that an intruder can send to a server system to perform some illegal activity. They are the hidden programs that allow identification of system vulnerabilities. Attackers can use botnets to perform the tedious tasks involved in probing a system for known vulnerabilities.

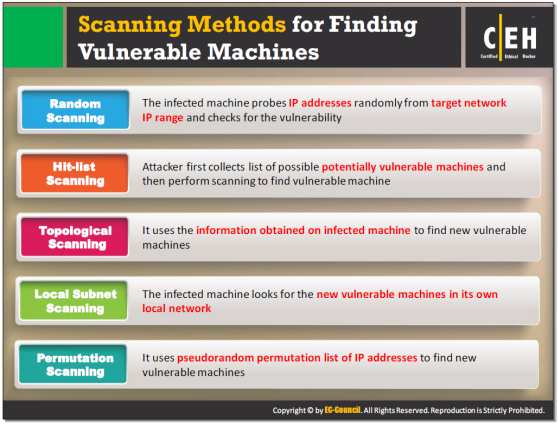
Attackers can use botnets to perform the following tasks:

- **Distributed denial-of-service attacks:** Botnets can generate DDoS attacks, which eat up the bandwidth of the victims' computers. Botnets can also overload a system, wasting valuable host system resources and destroying network connectivity.
- **Spamming:** Attackers use SOCKS proxy for spamming. They harvest email addresses from Web pages or some other sources.
- **Sniffing traffic:** A packet sniffer observes the data traffic entering a compromised machine. It allows an attacker to collect sensitive information such as credit card numbers and passwords. The sniffer also allows an attacker to steal information from one botnet and use it against another botnet. In other words, botnets can rob one another.
- **Keylogging:** Keylogging provides sensitive information, such as system passwords. Attackers use keylogging to harvest PayPal account login information.
- **Spreading new malware:** Botnets can be used to spread new bots.
- **Installing advertisement add-ons:** Botnets can be used to perpetrate "click fraud" by automating clicks.
- **Google AdSense abuse:** Some AdSense companies permit showing Google ads on their Web sites for economic benefits. This allows an intruder to automate clicks on an ad, thus producing a percentage increase in the click queue.
- **Attacking IRC chat networks:** Also called as clone attacks, these are similar to a DDoS attack. A master agent instructs each bot to link to thousands of clones within the IRC network, which can flood the network.
- **Manipulating online polls and games:** Every botnet has a unique address, enabling it to manipulate online polls and games.
- **Mass identity theft:** Botnets can produce a large number of e-mails pretending to be some reputable site such as eBay. This technique allows attackers to steal information for identity theft.

The diagram in the slide illustrates how an attacker launches a botnet-based DoS attack on a target server. The attacker sets up a bot Command and Control (C&C) Center. He/she then infects a machine (bot), and compromises it. Later on, they use this bot to infect and compromise other vulnerable systems available in the network, resulting in a botnet. The bots (also known as zombies) connect to the C&C center and waits for instructions. The attacker then sends malicious commands to the bots through the C&C center. Finally, as per the instructions given by the attacker, the bots launch DoS attack on a target server, making its services unavailable to the legitimate users in the network.







Discussed below are the scanning methods that an attacker uses to find vulnerable machines available in a network:

- **Random Scanning**

  In this technique, the infected machine (an attacker's machine or a zombie) probes IP addresses randomly from the target network IP range and checks their vulnerability. On finding a vulnerable machine, it breaks into it and tries to infect it by installing the same malicious code installed on it. This technique generates a significant traffic as many compromised machines probe and check the same IP addresses. Malware propagation takes place quickly in the initial stage and later on it reduces as the number of new IP addresses available will be less as the time passes.

- **Hit-list Scanning**

  Through scanning, an attacker first collects a list of potentially vulnerable machines, and then to create a zombie army, he/she performs scanning down the list to find a vulnerable machine. On finding one, the attacker installs a malicious code on it and divides the list in half. In one half, the attacker continues to scan; the other half is given to the newly compromised machine to find the vulnerable machine in its list and continue the same process as discussed before. This goes on simultaneously from an everlasting increasing number of compromised machines. This technique ensures installation of malicious code on all the potential vulnerable machines in the hit list within a short time.

- **Topological Scanning**

  This technique uses the information obtained from the infected machine to find new vulnerable machines. An infected host checks for URLs in the disk of a machine that it wants to infect. Then it shortlists the URLs, targets and checks their vulnerability. This technique yields accurate results and the performance is similar to the hit-list scanning technique.

- **Local Subnet Scanning**

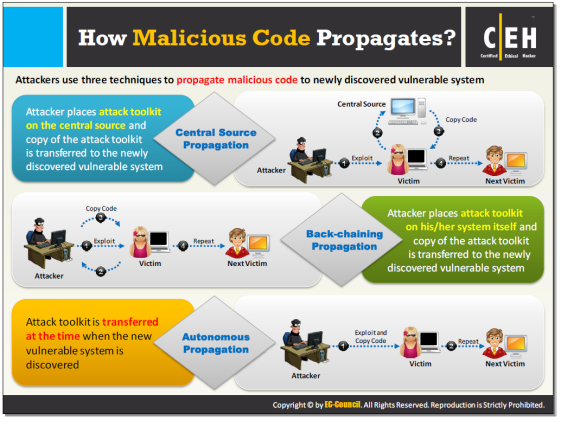
  The infected machine looks for new vulnerable machines in its local network, behind the firewall using the information hidden in the local addresses. Attackers use this technique in combination with other scanning mechanisms.

- **Permutation Scanning**

  In this technique, attackers share a common pseudorandom permutation list of IP addresses among all machines that is created by using a block cipher of 32 bits and a preselected key. If a compromised host has been infected either during hit-list scanning or local subnet scanning, it begins to scan just after its point in the permutation list and scans through the list to identify new targets. In case, if a compromised host is infected during permutation scanning, it starts scanning at a random point. If it encounters an already infected machine, then it chooses a new random start point in the permutation list and proceeds from there. The process of scanning stops when the compromised host encounters sequentially a pre-defined number of already infected machines failing to find the new targets. Now generate a new permutation key to initiate a new scanning phase.

  Advantages

  - Reinfection of the same target is avoided.
  - New targets are scanned at random (thus ensuring high scanning speed).



Discussed below are the three techniques that an attacker uses to propagate malicious code and build attack networks:

- **Central Source Propagation**

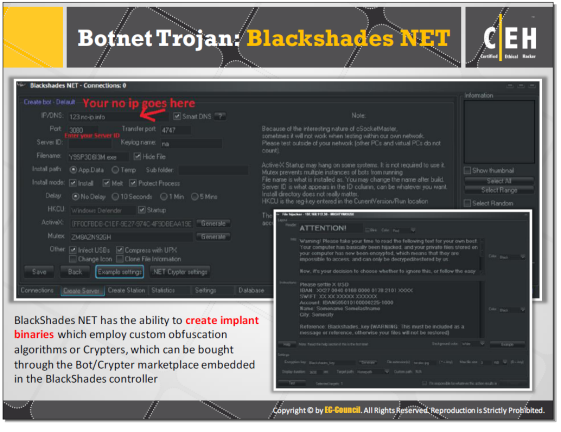
  In this technique, once the attacker finds a vulnerable machine, he/she instructs the central source to transfer a copy of the attack toolkit to the newly compromised machine, on which automatic installation of attack tools takes place, managed by a scripting mechanism. This initiates a new attack cycle, in which the newly infected machine looks for other vulnerable machine and repeats the same process to install the attack toolkit on it. In general, this technique uses HTTP, FTP, and RPC protocols.

- **Back-Chaining Propagation**

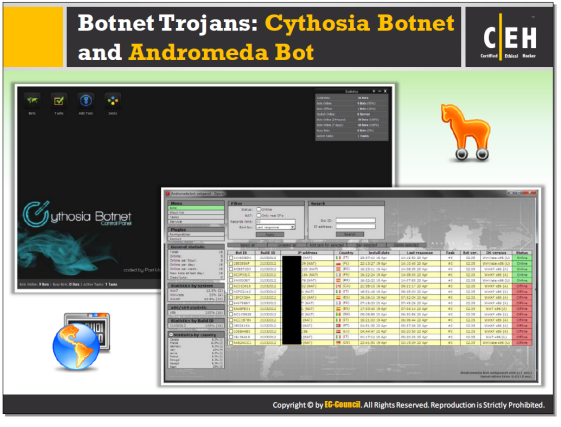
  In this technique, the attacker sends the attack toolkit to the newly compromised system. The attack tools installed on the attacking machine has some special methods to accept a connection from the compromised system and then transfer a file containing attack tools to it. Simple port listeners (which copy file contents) or full intruder-installed Web servers, both of which use the TFTP (Trivial File Transfer protocol) support this back-channel file copy.

- **Autonomous Propagation**

  Unlike previously mentioned mechanisms, which transfer the external file source to the attack toolkit, here the attacking host itself transfers the attack toolkit to the newly discovered vulnerable system, exactly at the time it breaks into that system.



BlackShades NET is a Remote Access Trojan, which allows an attacker the ability to view a victim's webcam, log their key strokes, steal their files, further infect a system with subsequent malware, hold the infected system for ransom and a slew of other functionality. It has multiple methods of unique concealment used to hide from antivirus engines by employing the use of custom "**crypters**" that obfuscates the implant binary. According to media reports, attackers recently used it against Syrian political activists.



Given below are the botnet Trojans:

Cythosia Botnet

Cythosia is a botnet with standard Botnet features. It is a common botnet for hijacking PC's and using them to perform DDoS attacks. It supports SYN flooding, UDP flooding, and HTTP flooding. It is customizable and modular.

Functionalities/Features:

- Download and Execute
- Update
- Distributed Denial of Service (DDoS) Functions

  Syn

  - 20 Bots can kill little Sites
  - Customizable Port & Strength (Http, SQL, and Gameserver)

  UDP

  - Perform attacks on home connections
  - Highly customizable

HTTP

- Multithreaded GET Requests – Generates heavy traffic
- Keeps GET Requests open

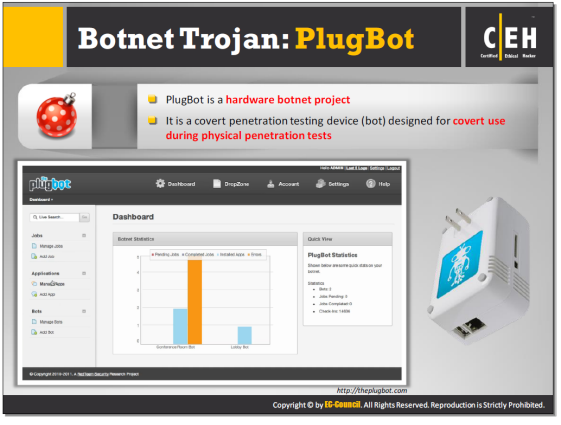
- Socks5 Proxy
  - Opens Port with UPnP if the router supports it
  - Redirects all TCP requests multithreaded
  - Configurable Username and Password
- Control Panel
  - Ajax Panel
  - Hardcoded Password -> secure
  - Task management System
  - Export Online SOCKS5 LIST

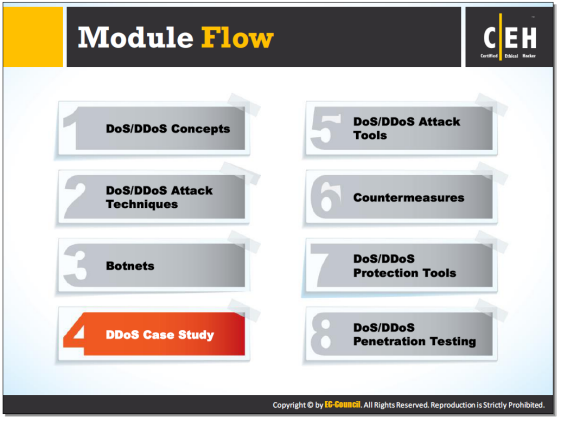
Andromeda Bot

The Andromeda botnet is a large botnet that uses a bot malware infection that allows criminals to control simultaneously thousands of infected computer systems.

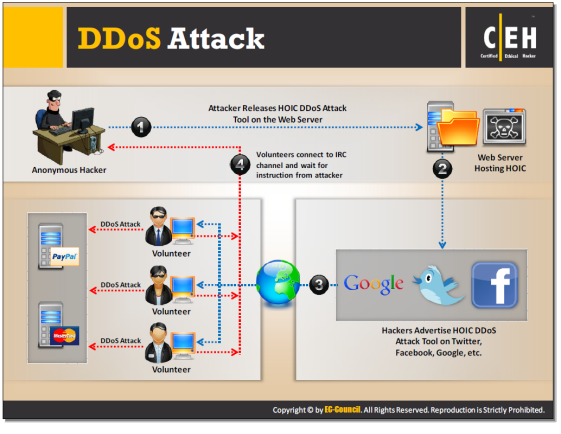
Some of the characteristics of Andromeda botnet:

- It can support any number of malicious domains, allowing criminals to expand indiscriminately.
- The exchanges between the infected computer and the Control and Command server are encrypted with RC4; this makes tough for PC security researchers catch these messages to know more about the criminal activities.
- The Andromeda malware employs a user-friendly console that allows criminals to keep detailed statistics of their attacks and the location and activities of all computer systems in the Andromeda botnet.





DDoS is a sophisticated and complex attack based on DoS attack and multiple distributed attack sources. In a DDoS attack, a large number of compromised computers (zombies) are involved to interrupt or suspend network services. This section deals with a DDoS case study.

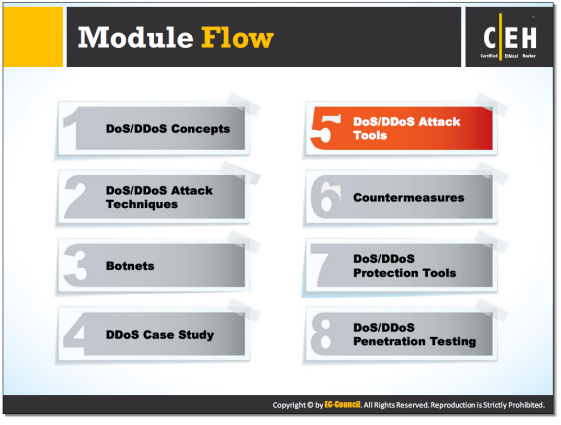


In a DDoS attack, attackers use a group of compromised systems (bots or zombies) usually infected with Trojans to perform a denial-of-service attack on a target system or network resource.

In the diagram above, an anonymous hacker hosts a HOIC DDoS attack tool on the webserver he/she owns or on any other compromised webserver. The hacker then advertises the HOIC DDoS attack tool on the social networking sites or on search engines such as Twitter, Facebook, and Google, providing a malicious download link to it in the ad.

Users who desire to perform the DDoS attack, may download the HOIC DDoS attack tool by clicking on the malicious link provided by the hacker. These users are termed "**volunteers**." All the volunteers connect via IRC channel to the anonymous hacker and await their instructions to proceed further. The hacker instructs the volunteers to flood the target web server (e.g., PayPal, MasterCard, PAYBACK) with multiple requests. On receiving their instructions, the volunteers take action accordingly, which results in the target server being overwhelmed. Thus, it will no longer respond to requests from even legitimate users.

Hackers advertise botnets on various blogs, search engines, social networking sites, and so on, providing download links for them. The intension in doing so is to spread the botnet and increase the size of the attack network. This method of attack is very quick and effective. Screenshots in the slide show some examples of the kind of ads that a hacker would host on the Internet to download botnets.



This section deals with various DoS/DDoS attack tools used to take over a single or multiple network machines to exhaust their computing resources or render them unavailable to their intended users.

DoS and DDoS Attack Tool: Pandora DDoS Bot Toolkit

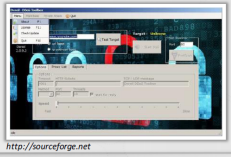
The Pandora DDoS Bot Toolkit is an updated variant of the **Dirt Jumper DDoS toolkit**

It offers five distributed denial of service **(DDoS) attack modes**

It generates five attack types:

- HTTP min
- HTTP download
- HTTP Combo
- Socket Connect
- Max Flood

DoS and DDoS Attack Tools: Dereil and HOIC



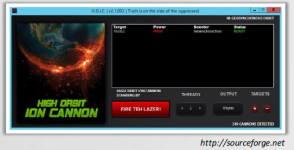
http://sourceforge.net

Dereil

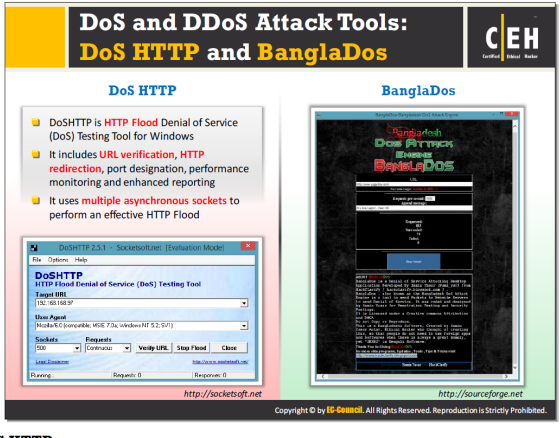
Dereil is professional (DDoS) Tools with modern patterns for attack via **TCP**, **UDP**, and **HTTP protocols**

HOIC

HOIC makes a DDoS attacks to **any IP address**, with a user selected port and a user selected protocol



http://sourceforge.net



DoS HTTP

Source: *http://www.socketsoft.net*

DoS HTTP works simultaneously on multiple clients to emulate a DDoS attack. It also allows IT professionals to test web server performance and evaluate its protection software.

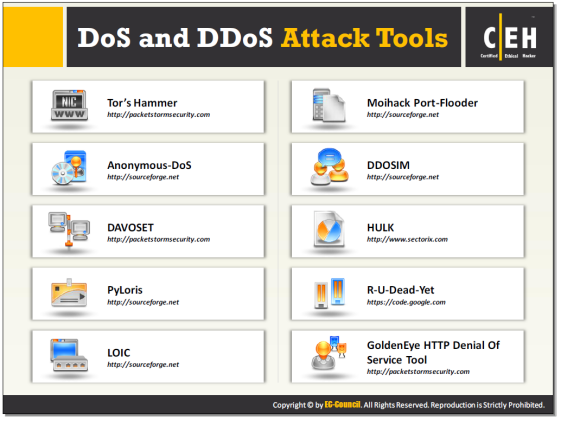
Features

- Supports HTTP redirection for automatic page redirection
- Includes URL verification that displays the response header and document
- Includes performance monitoring to track requests issued and responses received
- Allows customized User Agent header fields
- Uses multiple asynchronous sockets to perform an effective HTTP flood
- Allows user defined Socket and Request settings
- Supports numeric addressing for target URLs
- Allows multiple clients to emulate a Distributed Denial of Service (DDoS) Attack
- Allows target port designation within the URL [http://host:port/]
- Clears Target URLs and Resets All options

BanglaDos

Source: *http://sourceforge.net*

BanglaDos is an open-source network stress-testing and DoS attack application. Using BanglaDos, one can send thousands of garbage requests to web servers like visa.com and paypal.com to shut them down.



Discussed below are various DoS and DDoS attack tools:

Tor's Hammer

Source: *http://packetstormsecurity.com*

Tor's Hammer is a slow post DoS testing tool written in Python. It is capable to run through the Tor network to stay anonymous. If you are going to run it with Tor, it assumes you are running Tor on 127.0.0.1:9050. It kills most unprotected web servers running Apache and IIS via a single instance. It kills Apache 1.X and older IIS with ~128 threads, newer IIS and Apache 2.X with ~256 threads.

Anonymous-DoS

Source: *http://sourceforge.net*

Anonymous-DoS is a HTTP flood program written in HTA and JavaScript, designed to be lightweight, portable, possible to be uploaded to websites while still having a client version, and made for anonymous DDoS attacks. It will flood a chosen web server with HTTP connections, with enough it will crash the server, resulting in denial of service.

Features

- Powerful HTTP DoS attack
- Perfect for testing web servers
- Anonymous dedicated
- Multi-platform

DAVOSET

Source: *http://packetstormsecurity.com*

DAVOSET (DDoS attacks via other sites execution tool) is a tool for committing distributed denial of service attacks using execution on other sites.

There are two vulnerabilities that allow such attacks:

- Abuse of functionality (which allows to force one site to connect to arbitrary sites)
- Insufficient anti-automation (which allows to conduct such attacks in an automated fashion)

PyLoris

Source: *http://sourceforge.net*

PyLoris is a scriptable tool for testing a server's vulnerability to connection exhaustion denial of service (DoS) attacks. PyLoris can utilize SOCKS proxies and SSL connections, and can target protocols such as HTTP, FTP, SMTP, IMAP, and Telnet.

Features

- Tkinter GUI
- Scripting API
- Anonymity
- TOR Proxying
- SOCKS Proxying

LOIC

Source: *http://sourceforge.net*

LOIC is a network stress testing and DoS attack application. We can also call it an application-based DOS attack as it mostly targets web applications. We can use LOIC on a target site to flood the server with TCP packets, UDP packets, or HTTP requests with the intention of disrupting the service of a particular host.

Moihack Port-Flooder

Source: *http://sourceforge.net*

It is a TCP/UDP Port Flooder written in Python. One can use this tool to stress-test their network devices and measure router or server's load.

Features

- Target's address can be in both IPv4 and URL format
- Manual port selection
- Uses both TCP/UDP
- Smart recreation of socket objects
- Random-packet creation option available

DDOSIM

Source: *http://sourceforge.net*

DDOSIM (DDoS Simulator) simulates several zombie hosts (having random IP addresses) that create full TCP connections to the target server. After completing the connection, DDOSIM starts the conversation with the listening application (e.g., HTTP server).

Features

- Application-layer DDoS attacks
- TCP-based attacks
- Several zombies simulation
- Random-source IP addresses

HULK

Source: *http://www.sectorix.com*

HULK (Http Unbearable Load King) is a Web-server DoS tool. It generates volumes of unique and obfuscated traffic at a web server, bypassing caching engines and therefore hitting the server's direct resource pool.

R-U-Dead-Yet

Source: *https://code.google.com*

R-U-Dead-Yet, or RUDY for short, implements a generic HTTP DoS attack via long-form field submissions. It runs with an interactive console menu, automatically detecting forms in a given URL, and allowing the user to choose which forms and form fields are desirable to use for the POST attack. In addition, the tool offers unattended execution by providing the necessary parameters within a configuration file. In version 2.x, RUDY supports SOCKS proxies and session persistence using cookies, when available.

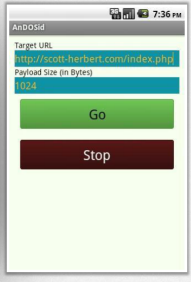
GoldenEye HTTP Denial Of Service Tool

Source: *http://packetstormsecurity.com*

GoldenEye is an HTTP/S Layer 7 denial of service testing tool. It uses KeepAlive (and Connection: keep-alive) paired with Cache-Control options to persist socket connection breaking through caching (when possible) until it consumes all available sockets on the HTTP/S server.

DoS and DDoS Attack Tool for Mobile: AnDOSid

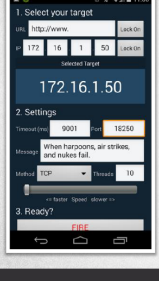
- AnDOSid allows attacker to simulate a **DOS attack** (A http post flood attack to be exact) and **DDoS attack on a web server** from mobile phones

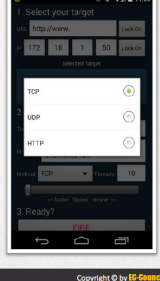


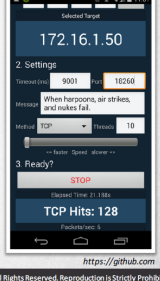
http://andosid.android.informer.com

DoS and DDoS Attack Tool for Mobile: Low Orbit Ion Cannon (LOIC)

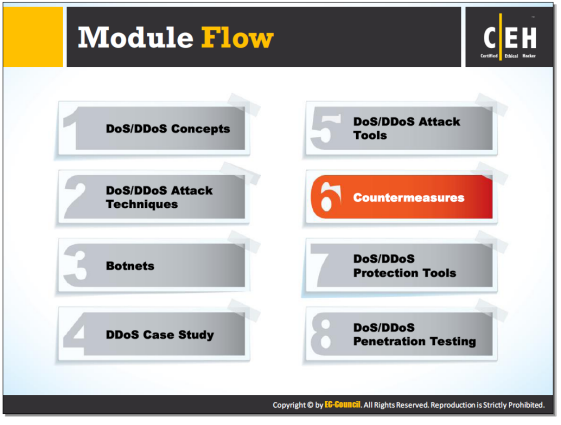
- Android version of Low Orbit Ion Cannon (LOIC) software is used for **flooding packets** which allows attacker to **perform DDoS attack** on target organization



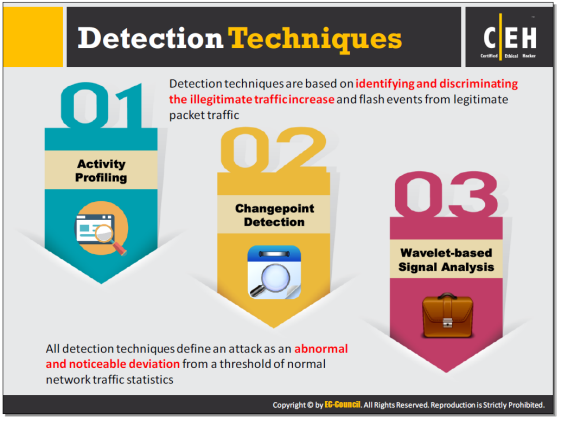




https://github.com



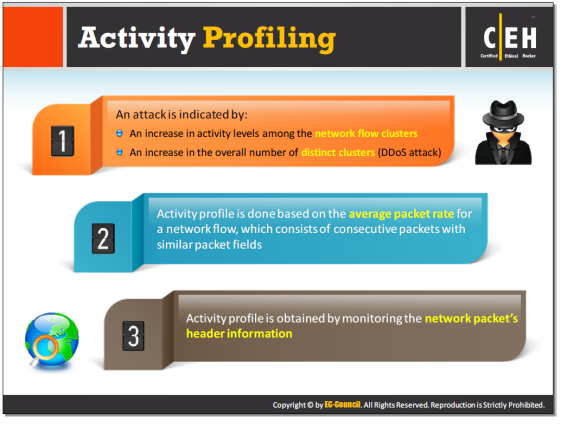
DoS/DDoS is one of the foremost security threats on the Internet, thus there is a greater necessity for solutions to mitigate these attacks. This section deals with detection methods, various preventive measures, and response to DoS/DDoS attacks.



Early detection techniques help to prevent DoS/DDoS attacks. Detecting a DoS/DDoS attack is a tricky job. A DoS/DDoS attack traffic detector needs to distinguish between a genuine and a bogus data packet, which is not always possible; the techniques employed for this purpose are not perfect. There is always a chance of confusion between traffic generated by a legitimate network user and traffic generated by a DoS/DDoS attack.

One problem in filtering bogus traffic from legitimate traffic is the volume of traffic. It is impossible to scan each data packet to ensure security from a DoS/DDoS attack.

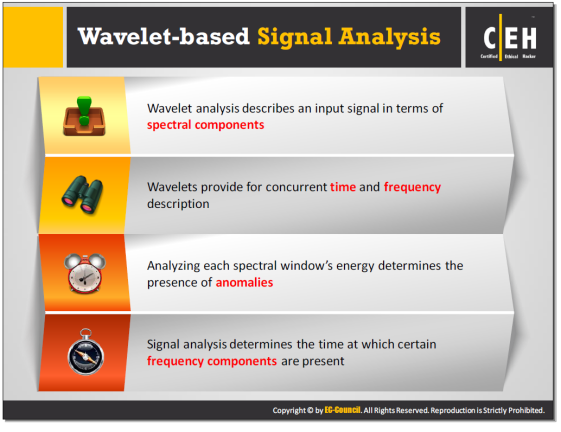
All the detection techniques used today to define an attack as an abnormal and noticeable deviation in network traffic characteristics. These techniques involve statistical analysis of deviations to categorize malicious and genuine traffic.



An activity profile is the average packet rate of data packets with similar packet header information. Packet header information includes the destination and sender IP addresses, ports, and transport protocols used.

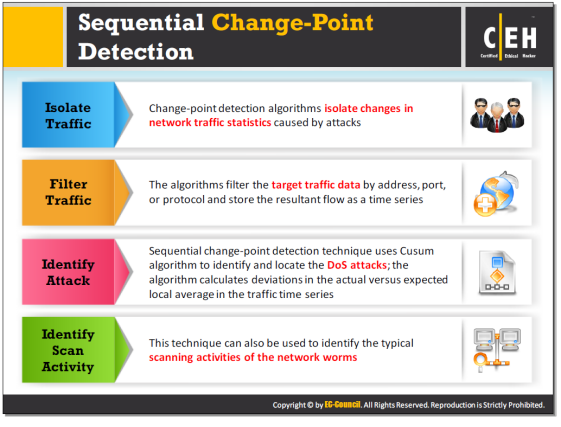
The higher a flow's average packet rate or activity level, the less time there is between consecutive matching packets. Randomness in average packet rate or activity level can indicate suspicious activity. The entropy calculation method measures randomness in activity levels. If the network is under attack, entropy of network activity levels will increase.

One of the major hurdles for an activity profiling method is the volume of the traffic. This problem can be overcome by clustering packet flows with similar characteristics. DoS attacks generate a large number of data packets that are very similar, so an increase in the average packet rate or an increase in the diversity of packets could indicate a DoS attack.



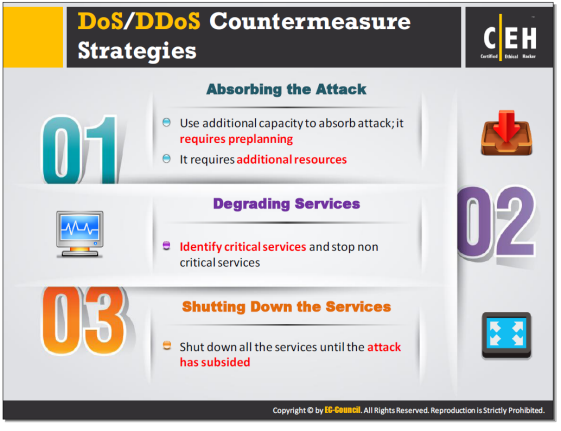
The wavelet analysis technique analyzes network traffic in terms of spectral components. It divides incoming signals into various frequencies and analyzes different frequency components separately. These techniques check for certain frequency components present at a specific time and provide a description of those components. Presence of an unfamiliar frequency indicates suspicious network activity.

A network signal consists of a time-localized data packet flow signal and background noise. Wavelet-based signal analysis filters out the anomalous traffic flow input signals from background noise. Normal network traffic is generally low-frequency traffic. During an attack, the high-frequency components of a signal increase.



The sequential change-point detection technique filters network traffic by IP addresses, targeted port numbers, and communication protocols used, and stores the traffic flow data in a graph that shows the traffic flow rate versus time. Sequential change-point detection algorithms highlight any change in traffic flow rate. If there is a drastic change in traffic flow rate, a DoS attack may be occurring.

This technique uses **Cumulative Sum** (Cusum) algorithm to identify and locate the DoS attacks; the algorithm calculates deviations in the actual versus expected local average in the traffic time series. The sequential change-point detection technique identifies the typical scanning activities of the network worms.



Discussed below are the DoS/DDoS countermeasure strategies:

- **Absorb the Attack**

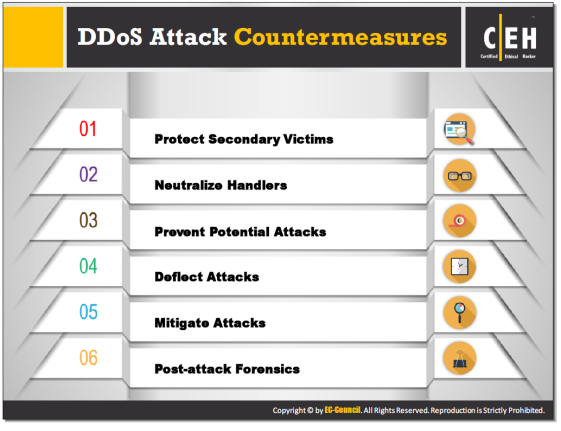
  Use additional capacity to absorb the attack; it requires preplanning. It also requires additional resources. One disadvantage associated is the cost of additional resources, even when no attacks are under way.

- **Degrading Services**

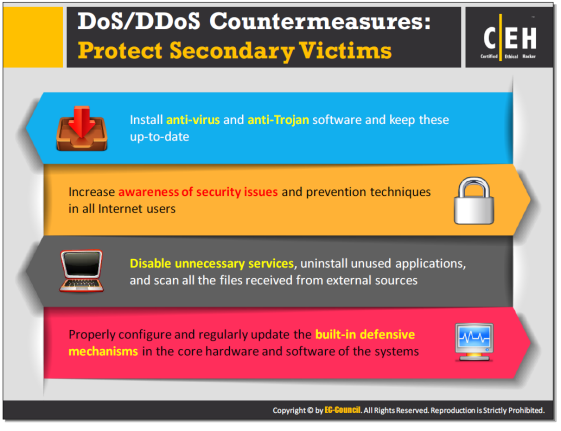
  If it is not possible to keep all your services functioning during an attack, it is a good idea to keep at least the critical services functional. For this, first identify the critical services and then customize the network, systems, and application designs in such a way to cut down the noncritical services. This may help you to keep the critical services functional.

- **Shutting Down the Services**

  Simply shut down all services until an attack has subsided. Though it may not be an ideal choice, it may be a reasonable response in some cases.



There are many proposed solutions for mitigating the effects of a DDoS attack. However, no single complete solution exists that can provide protection against all known forms of DDoS attacks. Moreover, attackers are continually devising with new ways to perform DDoS attacks in order to bypass security solutions employed.



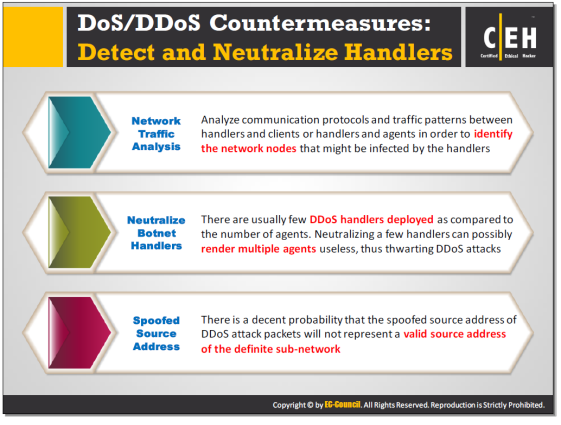
Individual Users

The best method to prevent DDoS attacks is for secondary victim systems to prevent themselves from taking part in the attack. This demands intensified security awareness and prevention techniques. Secondary victims must monitor their security on regular basis to remain protected from DDoS agent software. They must ensure that the system does not install a DDoS agent program and that they are not transferring DDoS agent traffic into the network.

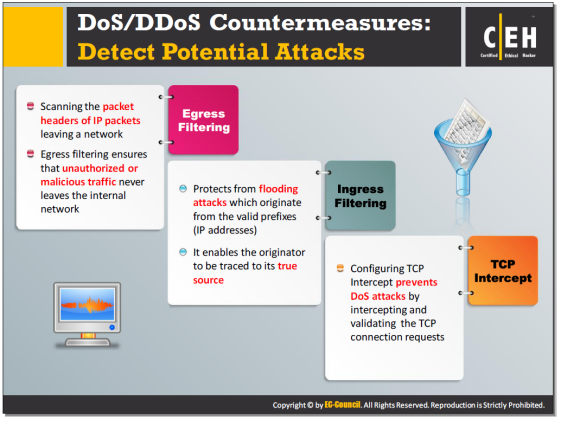
Anti-virus and Anti-Trojan software must be installed and updated on a regular basis, as well as software patches to fix known vulnerabilities. It is important to disable unnecessary services, uninstall unused applications, and scan all files received from external sources. Because these tasks may appear daunting to the average Web surfer, the core hardware and software of computing systems come with integrated mechanisms that defend against malicious code insertion. Employing the above countermeasures will leave attackers with no DDoS attack network from which they can launch DDoS attacks.

Network Service Providers

Service providers and network administrators can enter dynamic pricing (altering price) for their network usage to encourage potential secondary victims and charge them for accessing the Internet to become more active in preventing themselves from becoming part of a DDoS attack.



An important method used to stop DDoS attacks is to detect and neutralize handlers. In the agent-handler DDoS attack-tool arsenal, the handler works as an intermediary for the attacker to initiate the attacks. Discovering the handlers in the network and disabling them can be a quick method of disrupting the DDoS attack network. Because there are few DDoS handlers deployed in the network, as compared to the number of agents, neutralizing a few handlers can possibly render multiple agents useless, thus thwarting DDoS attacks. To stop DDoS attacks, a thorough comprehension of communication protocols and traffic patterns between handlers and agents or handlers and clients, to detect network nodes infected with a handler.



Ingress Filtering

Ingress filtering is a packet filtering technique used by many Internet Service Providers (ISPs) to prevent source address spoofing of Internet traffic, and thus indirectly combat several types of net abuse by making Internet traffic traceable to its true source. It protects against flooding attacks that originate from valid prefixes (IP addresses).

Egress Filtering

Organizations can establish a number to help in detecting potential attacks. Egress filtering scans the headers of IP packets going out of network. If the packets pass the specifications, they can route out of the sub-network from which they originated. The packets will not reach the targeted address if they do not meet the necessary specifications.

DDoS attacks generate spoofed IP addresses. Establishing protocols to require any legitimate packet that leaves a company's network to have a source address where the network portion matches the internal network can help mitigate attacks. A properly developed firewall for the sub-network can filter out many DDoS packets with spoofed IP source addresses.

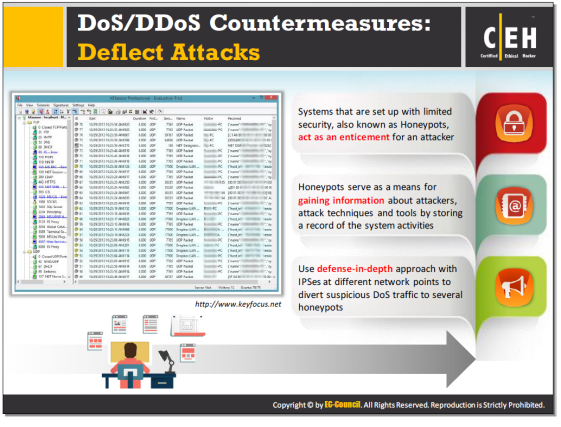
If a Web server is vulnerable to a zero-day attack known only to the underground hacker community, even after applying if all available patches to the server, a server can still be vulnerable. However, if user enables egress filtering, they can save the integrity of a system by keeping the server from establishing a connection back to the attacker. This would also limit the effectiveness of many payloads used in common exploits. Outbound exposure can be restricted

to required traffic only, thus limiting the attacker's ability to connect to other systems and gain access to tools that can enable further access into the network.

TCP Intercept

TCP intercept is a traffic-filtering feature in routers to protect TCP servers from a TCP SYN-flooding attack, a kind of DoS attack. In a SYN-flooding attack, the attacker sends a huge volume of requests for connections with unreachable return addresses. As the addresses are not reachable, the connections cannot be established and remain unresolved. This huge volume of unresolved open connections overwhelms the server and may cause it to deny service even to valid requests. Consequently, legitimate users may not be able to connect to a website, access email, use the FTP service, and so on.

In TCP intercept mode, the router intercepts the SYN packets sent by the clients to the server and matches with an extended access list. If there is a match, then on behalf of the destination server, the intercept software establishes a connection with the client. Similarly, the intercept software also establishes a connection with the destination server on behalf of the client. Once the two half connections are established, the intercept software combines them transparently. Thus, the TCP intercept software prevents the fake connection attempts from reaching the server. The TCP intercept software acts as a mediator between the server and the client throughout the connection.



Honeypots are systems that are only partially secure and thus serve as lures to attackers. Recent research reveals that a honeypot can imitate all aspects of a network, including its Web servers, mail servers, and clients. Honeypots are intentionally set up with low security to gain the attention of the DDoS attackers. A honeypot attracts DDoS attackers, in that they will install handlers or agent code within the honeypot. This avoids compromising of more-sensitive systems. Honeypots not only protect the actual system from attackers, but also keep track of details about what the attackers are doing by storing the information in a record. This gives the owner of the honeypot a way to keep a record of handler and/or agent activity. Users can use this knowledge for defending against any future DDoS installation attacks.

There are two different types of honeypots:

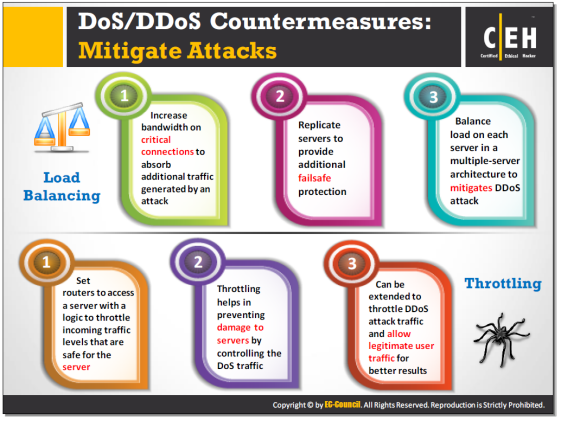
- Low-interaction honeypots
- High-interaction honeypots

An example of high-interaction honeypots is a honeynet. Honeynets are the infrastructure—in other words, they simulate the complete layout of an entire network of computers—but they are originally for "capturing" attacks. The goal is to develop a network wherein all activities are controlled and tracked. This network contains potential victim decoys, and the network even has real computers running real applications.

KFSensor

Source: *http://www.keyfocus.net*

KFSensor is a Windows-based honeypot Intrusion Detection System (IDS). It acts as a honeypot to attract and detect hackers and worms by simulating vulnerable system services and Trojans. By acting as a decoy server, it can divert attacks from critical systems and provide a higher level of information than can be achieved by using firewalls and NIDS alone. Above is a snapshot of KFSensor Professional.



Load Balancing

Bandwidth providers can increase their bandwidth on the critical connections in case of a DDoS attack to prevent their servers from going down. Using a replicated server model provides additional failsafe protection. Replicated servers help in better load management (balancing loads on each server in a multiple-server architecture), increase both normal network performance, and mitigate the effect of a DDoS attack.

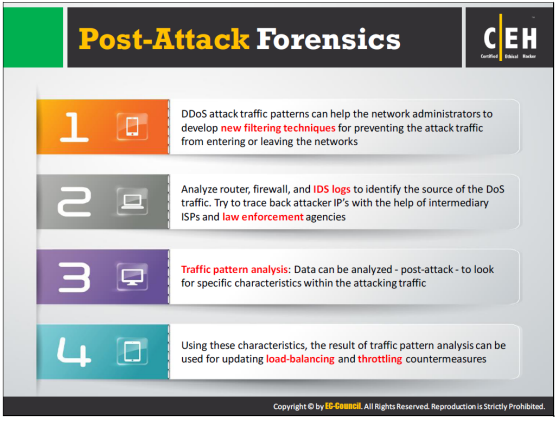
Throttling

"Min-max fair server-centric router" throttles (minimum and maximum throughput controls) help users prevent their servers from going down. This method helps routers manage heavy incoming traffic, so that the server can handle it. It filters legitimate user traffic from fake DDoS attack traffic.

The major limitation with this method is that it may trigger false alarms. Sometimes, it may allow malicious traffic to pass while dropping some legitimate traffic.

Drop Requests

Another method is to drop packets when a load increases; usually the router or server does it. On the other hand, system induces requester to drop the request by making to solve a difficult puzzle that requires a lot of memory or computing power, before continuing with the request. This will let users of zombie systems to find performance degradation, and could possibly stop them from taking part in transferring DDoS attack traffic.



Traffic Pattern Analysis

During a DDoS attack, the traffic pattern tool stores post attack data, which users analyze for the special characteristics of the attacking traffic. These data are helpful in updating load balancing and throttling countermeasures to enhance their efficiency and protection ability. Moreover, DDoS attack traffic patterns can help network administrators to develop new filtering techniques for hindering DDoS attack traffic from entering or leaving their networks. Analyzing DDoS traffic patterns can also help network administrators to ensure that an attacker cannot use their servers as a DDoS platform to break into other sites.

Run the Zombie Zapper Tool

One important method is the Zombie Zapper tool. When a company is unable to ensure the security of its servers and a DDoS attack starts, the network IDS (Intrusion Detection System) notices the high volume of traffic that indicates a potential problem. The targeted victim can run Zombie Zapper to stop the packets from flooding the system.

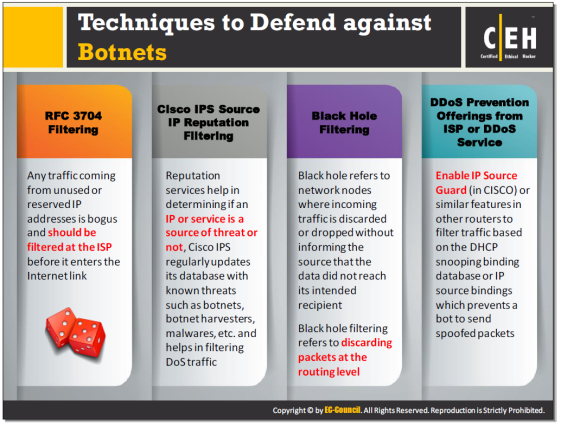
There are two versions of Zombie Zapper. One runs on UNIX, and the other runs on Windows systems. Currently, this tool acts as a defense mechanism against Trinoo, TFN, Shaft, and Stacheldraht. Like the scanning programs, it also assumes that the user has installed the on the default ports with default passwords.

Packet Traceback

Packet traceback refers to tracing back attack traffic. Packet Traceback is similar to reverse engineering. The targeted victim works backwards by tracing the packet to its original source. Once the victim identifies the true source, he or she can take necessary steps to block further attacks from that source by developing necessary preventive techniques. In addition, Packet Traceback can assist in gaining knowledge regarding the various tools and techniques that an attacker uses. This information can be of help in developing and implementing different filtering techniques to block the attack.

Event Logs

DDoS event logs assist in forensic investigation and the enforcement of laws. This is helpful when an attacker causes destruction resulting in severe financial damage. The providers can use honeypots and other network security mechanisms such as firewalls, packet sniffers, and server logs to store all the events that have taken place during the setup and execution of the attack. This allows network administrators to recognize the type of DDoS attack or a combination of attacks used.



There are four ways to defend against botnets:

- **RFC 3704 Filtering**

  RFC 3704 is a basic ACL filter. This filter requires packets sourced from valid, allocated address space, consistent with the topology and space allocation. A "**bogon list**" consists of all unused or reserved IP addresses that should not come in from the Internet. If any one of the IP address from the bogon list appears, it means that a spoofed source IP and the filter should drop it. Check with the ISP if they do RFC 3704 filtering for you in the cloud before the bogus traffic enters your Internet connection. The bogon list changes regularly, so, in case the ISP does not filter, then one has to manage one's own bogon ACL rules or switch to another ISP.

- **Black-Hole Filtering**

  Black-hole filtering is a common technique to defend against botnets and thus to prevent DoS attacks. Black hole refers to network nodes where incoming traffic is discarded or dropped without informing the source that the data did not reach the intended recipient. You can drop the undesirable traffic before it enters your protected network with a technique called Remotely Triggered Black-Hole Filtering, i.e., RTBH. As this is a remotely triggered process, you need to conduct this filtering in conjunction with your ISP. It uses BGP (Border Gateway Protocol) host routes to route traffic heading to victim servers to a "null0" next hop.

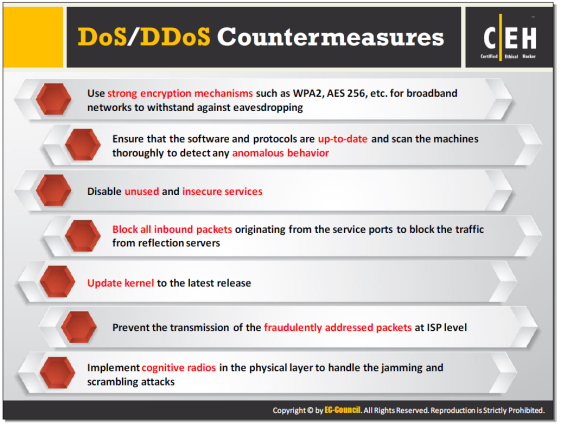
- **DDoS Prevention Offerings from ISP or DDoS Service**

  This method is effective in preventing IP-spoofing at the ISP level. Here, the ISP scrubs/cleans the traffic prior to allowing it to enter your Internet link. Since this service runs in the cloud, DDoS attack does not saturate your Internet links. In addition, some third parties offer cloud DDoS prevention services.

  One can enable IP Source Guard (in CISCO) or similar features in other routers to filter traffic based on the DHCP snooping binding database or IP source bindings which prevents a bot to send spoofed packets.

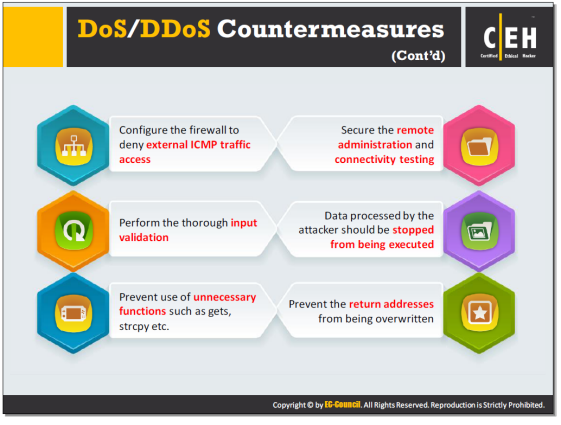
- **Cisco IPS Source IP Reputation Filtering**

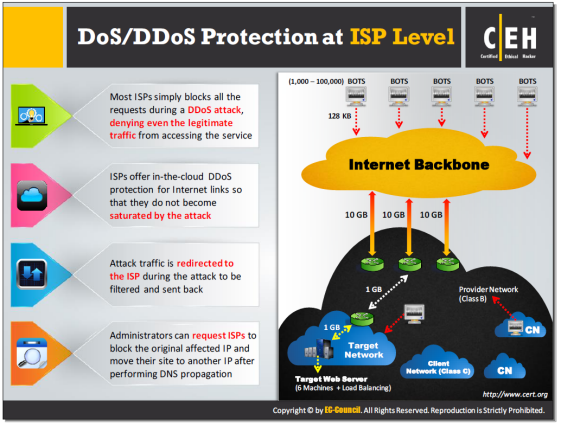
  Reputation services help in determining if an IP or service is a source of threat or not. Cisco Global Correlation, a new security capability of Cisco IPS 7.0, uses immense security intelligence. The Cisco SensorBase Network contains all the information about known threats on the Internet such as botnets, malware outbreaks, dark nets, and botnet harvesters. The Cisco IPS makes use of this network to filter DoS traffic before it damages critical assets. To detect and prevent malicious activity even earlier, it incorporates the global threat data into its system.



Implementing defensive mechanisms in appropriate places and following proper measures allows the heightening of organizational network security. Below is a list of countermeasures for combatting DoS/DDoS attacks:

- Use strong encryption mechanisms such as WPA2 and AES 256 for broadband networks to withstand against eavesdropping.
- Ensure that the software and protocols are up-to-date, and scan the machines thoroughly to detect any anomalous behavior.
- Disable unused and insecure services.
- Block all inbound packets originating from the service ports to block the traffic from reflection servers.
- Update kernel to the latest release.
- Enable TCP SYN cookie protection.
- Prevent the transmission of fraudulently addressed packets at the ISP level.
- Implement cognitive radios in the physical layer to handle jamming and scrambling attacks.

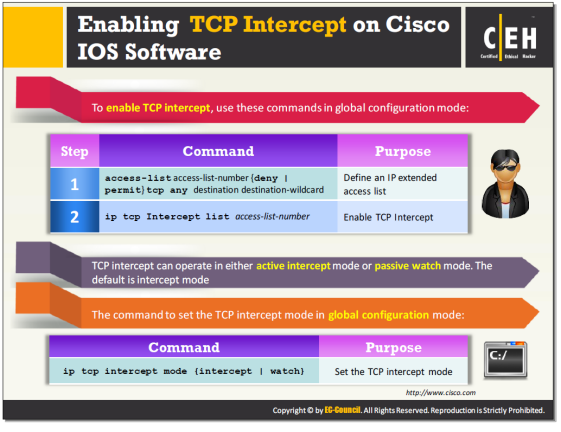




One of the best ways to defend against DoS attacks is to block them at the gateway. This happens by the contracted ISP. Many ISP's offer a "**clean pipes**" service-level agreement that promises to an assured bandwidth of genuine traffic rather than just total bandwidth of all traffic. If an ISP does not provide clean-pipes services, opt for subscription services provided by many cloud service providers. The subscription services serve as an intermediary, receive traffic destined for the network, filter it, and then pass on only trusted connections. Vendors such as Imperva, VeriSign, etc. offer services for cloud protection against DoS attacks.

Most ISPs simply block all requests during a DDoS attack, denying even legitimate traffic from accessing the service. ISPs offer in-the-cloud DDoS protection for Internet use to avoid saturation by the attack. The in-the-cloud DDoS protection redirects attack traffic to the ISP during the attack and sends it back. Administrators can request ISPs to block the original affected IP and move their site to another IP after performing DNS propagation.

Source: *http://www.cert.org*



One can enable TCP intercept by executing the commands given below in global configuration mode:

	Command	Purpose
Step 1	`access-list access-list-number {deny | permit} tcp any destination destination-wildcard`	Defines an IP extended access list
Step2	`ip tcp intercept list access-list-number`	Enables TCP intercept

TABLE 9.1: Steps to enable TCP Intercept on Cisco IOS

An access list achieves three purposes:

1. Intercepts all requests
2. Intercepts only those coming from specific networks
3. Intercepts only those destined for specific servers

Typically, the access list defines the source as any and the destination as specific networks or servers. As it is not important to know who to intercept packets from, do not filter on the source addresses. Rather, you identify the destination server or network to protect. TCP intercept can operate in either active intercept mode or passive watch mode. The default is intercept mode.

In the active intercept mode, the Cisco IOS software actively intercepts all inbound connection requests (SYN) and replies with a SYN-ACK on behalf of the server, then waits for an acknowledge (ACK) from the client. On receiving the ACK from the client, the server sends the original SYN and the software makes a three-way handshake with the server. Once the three-way handshake is complete, the two half connections are linked.

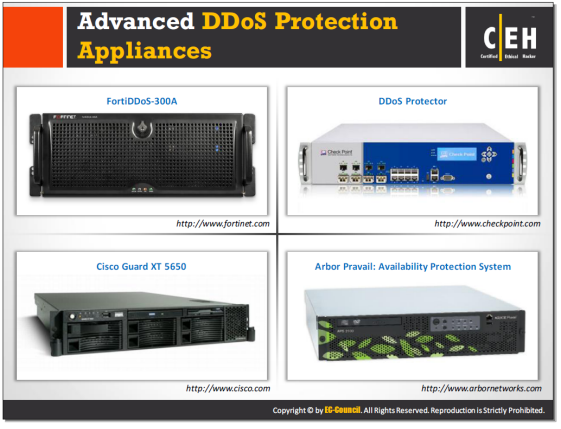
In the passive watch mode, the user sends connection requests that pass through the server but he or she needs to wait and watch until the connection is established. If connection requests fail to establish within 30 seconds, the software sends a reset request to the server to clear up its state.

The command to set the TCP intercept mode in global configuration mode:

Command	Purpose
`ip tcp intercept mode {intercept | watch}`	Set the TCP intercept mode

TABLE 9.2: Command to set the TCP intercept mode in global configuration mode

Source: *http://www.cisco.com*



Discussed below are some appliances that provide advanced protection against DDoS attacks.

FortiDDoS-300A

Source: *http://www.fortinet.com*

FortiDDoS provides comprehensive protection against DDoS attacks. It helps you protect your Internet infrastructure from threats and service disruptions by surgically removing network and application layer DDoS attacks, while letting legitimate traffic flow without being impacted.

DDoS Protector

Source: *http://www.checkpoint.com*

Check Point DDoS Protector appliances block DDoS attacks with multi-layered protection.

Benefits

- Blocks a wide range of attacks with customized multi-layered protection
  - Behavioral protection base-lining multiple elements and blocking abnormal traffic
  - Automatically generated and pre-defined signatures
  - Using advanced challenge/response techniques
- Fast response time—protects against attacks within seconds
  - Automatically defends against network flood and application layer attacks

- Customized protection optimized to meet specific network environment and security needs
- Quickly filters traffic before it reaches the firewall to protect networks, servers, and block exploits

- Flexible deployment options to protect any business
- Integrated with Check Point Security Management

Cisco Guard XT 5650

Source: http://www.cisco.com

The Cisco Guard XT 5650 is a DDoS mitigation appliance from Cisco Systems. Based on unique multi-verification process (MVP) architecture, the Cisco Guard XT employs the most advanced anomaly recognition, source verification, and anti-spoofing technologies to identify and block individual attack flows while allowing legitimate transactions to pass.

Benefits

- Multistage verification
- Multi-Gigabit performance
- Multilevel monitoring and reporting

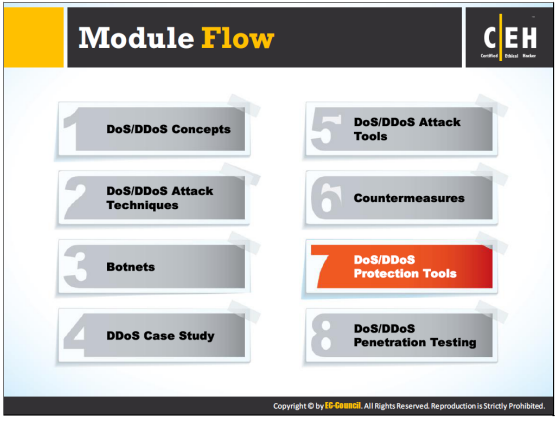
Arbor Pravail: Availability Protection System

Source: http://www.arbornetworks.com

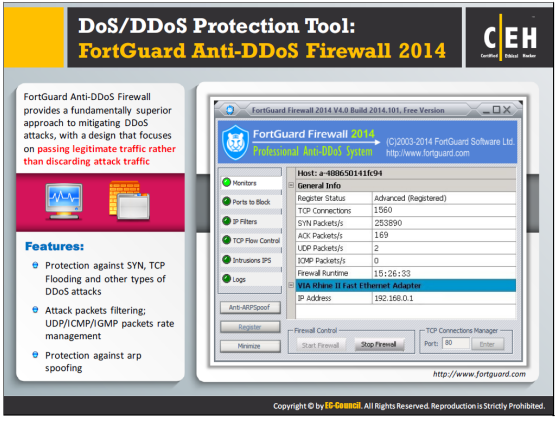
The Arbor Pravail's Availability Protection System ensures reliable access to your key network services by detecting and blocking external threats such as DDoS and other cyber-attacks before they escalate into costly service outages.

Features

- Custom protection with immediate blocking
- Proactive DDoS detection and mitigation
- Combined on-premise and cloud-based DDoS protection
- Built-in SSL inspection to block encrypted traffic
- Inbound reputation-based DDoS protection
- Inbound and outbound advanced threat protection



This section deals with various DoS/DDoS protection tools such as FortGuard Anti-DDoS Firewall, NetFlow Analyzer, WANGuard Sensor, and others that safeguard networks from DoS/DDoS attacks.

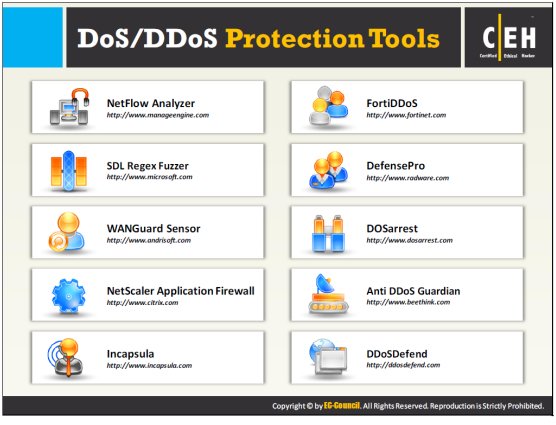


FortGuard Anti-DDoS Firewall provides a fundamentally superior approach to mitigating DDoS attacks, with a design that focuses on passing legitimate traffic rather than discarding attack traffic, handles the worst possible attack scenarios without performance degradation, and protects every distinct part of a network to avoid the collateral damage normally incurred.

Features

- Built-in intrusion prevention system
- Protection against SYN, TCP flooding, and other types of DDoS attacks
- Real-time visibility of attack packets
- TCP flow control (maximum connections restriction, per IP)
- Attack packets filtering; UDP/ICMP/IGMP packets rate management
- IP blacklist and whitelist
- Disable/enable proxy access on the application layer
- Protection against ARP spoofing
- Compact and comprehensive log records

Source: http://www.fortguard.com



Listed below are various DoS/DDoS protection tools:

NetFlow Analyzer

Source: *http://www.manageengine.com*

NetFlow Analyzer is a web-based bandwidth monitoring tool that performs in-depth traffic analysis using exported NetFlow data. NetFlow technology provides granular details about network traffic that have passed through an interface. NetFlow Analyzer processes this information to show you what applications are using bandwidth, who is using them, and when.

Features

- Bandwidth Monitoring
- Network Traffic Analytics
- Monitor traffic in routers/switches
- Reports—Consolidated, Custom, Troubleshoot
- Department wise bandwidth monitoring
- Application-specific usage monitoring
- Cisco Medianet and WAAS reporting
- Cisco AVC (Application visibility and control) monitoring
- Router traffic monitoring

SDL Regex Fuzzer

Source: http://www.microsoft.com

SDL Regex Fuzzer is a tool to help test regular expressions for potential DoS vulnerabilities in the Microsoft Security Development Lifecycle (SDL). To cause a DoS, attackers can exploit regular expression patterns containing certain clauses that execute in exponential time (for example, grouping clauses containing repetition that are themselves repeated).

WANGuard Sensor

Source: http://www.andrisoft.com

The WANGuard Sensor (Sniffing Sensor or Flow Sensor) provides incoming and outgoing traffic monitoring and accounting, as well as traffic anomalies detection. It adds advanced DDoS detection and DDoS mitigation capabilities. It protects networks and critical services against DDoS and other "volumetric" attacks by scrubbing off malicious packets with dynamic filtering rules applied to software or hardware firewalls for inline or redirected traffic.

NetScaler Application Firewall

Source: http://www.citrix.com

Citrix® NetScaler AppFirewall™ is a comprehensive ICSA certified web application security solution that blocks known and unknown attacks against web and web services applications. NetScaler AppFirewall enforces a hybrid security model that permits only correct application behavior, efficiently scans, and protects known application vulnerabilities. It analyzes all bi-directional traffic, including SSL-encrypted communication, to protect against a broad range of security threats without any modification to applications. It provides protection against data theft and layers 4–7 DoS attacks.

Incapsula

Source: http://www.incapsula.com

Incapsula protects applications and infrastructure against all types of DDoS threats. These include network-based attacks (e.g., Slowloris, ICMP or TCP and UDP floods) as well as application layer attacks (e.g., GET flood) that attempt to overwhelm server resources. Supporting Unicast and Anycast technologies, the service leverages a many-to-many defense methodology, automatically detecting and mitigating advanced DDoS attacks that exploit application and Web server vulnerabilities, hit-and-run DDoS events, and large botnets.

FortiDDoS

Source: http://www.fortinet.com

The FortiDDoS family of purpose-built appliances provides real-time visibility into the networks in addition to detection and prevention of DDoS attacks. It helps to protect Internet-facing infrastructure from threats and service disruptions by surgically removing network and application-layer DDoS attacks. One can defend their critical on-premises and cloud infrastructure from attacks while relying on sophisticated filtering technologies to allow legitimate traffic to continue to flow.

DefensePro

Source: http://www.radware.com

Radware's DefensePro is a behavior-based attack mitigation device that protects the infrastructure against network and application downtime, application vulnerability exploitation, malware spread, network anomalies, information theft, and other emerging cyber-attacks.

It provides security, including DDoS mitigation and SSL-based protection for applications and networks against known and emerging network security threats such as DoS and DDoS attacks, Internet pipe saturation, attacks on login pages, attacks behind CDNs, and SSL-based flood attacks.

DOSarrest

Source: http://www.dosarrest.com

DOSarrest's DDoS protection service protects websites from DDoS attacks. It secures websites from a large-volume UDP type flood, TCP SYN attack, or any other layer 7 attack. It has a network monitoring service called "DEMS" (DOSarrest External Monitoring Service), made up to eight sensors geographically distributed. Each sensor performs the following:

- Resolve domain name from the DNS
- TCP Connect, HTTP execution, HTTP first byte down load, HTTP Transfer
- Content change
- Calculates % uptime/downtime for any time period
- SSL Cert expiration notice (10 Days)

Anti DDoS Guardian

Source: http://www.beethink.com

Anti DDoS Guardian is high performance Anti DDoS software for Windows Servers. It manages network flow and keeps attacking traffic out. Anti DDoS Guardian protection can deal with most DDoS/DoS attacks, including Windows Remote Desktop brute-force password-guessing attacks, SYN attacks, IP flood, TCP flood, UDP flood, ICMP flood, and slow HTTP DDoS attacks. The Anti DDoS firewall limits network flow number, client bandwidth, client TCP connection number, UDP/ICMP packet rates, and most importantly, it controls the TCP half-open connection, which is effective in stopping SYN attacks.

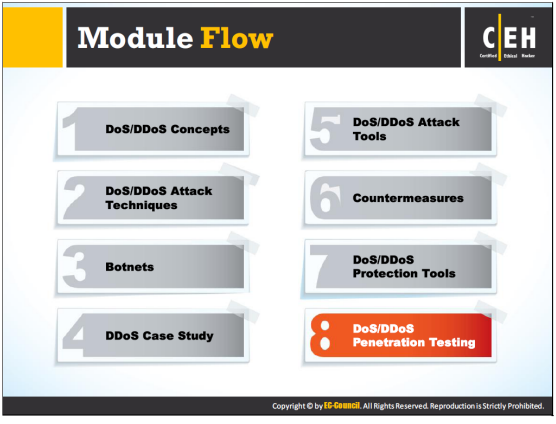
DDoSDefend

Source: http://ddosdefend.com

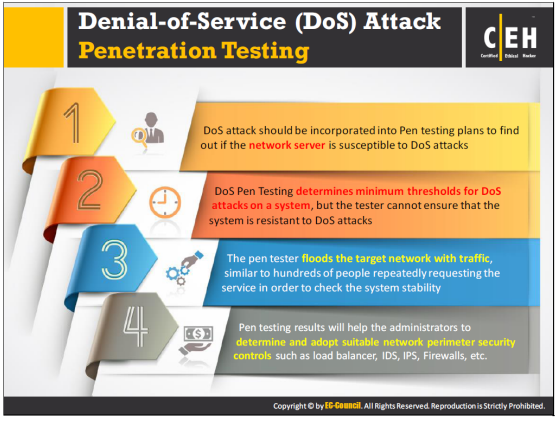
DDoSDefend is a DDoS protection service that protects websites from network and application-level DDoS attacks. It automatically detects and filters most types of attacks. It filters TCP, UDP, ICMP, and HTTP packets, and assures privacy and anonymity. DDoSDefend blocks malicious traffic and passes only legitimate traffic to websites. It acts as a load balancer in balancing filtered traffic between back-end servers.

Features

- Network Level DDoS Protection
- Basic HTTP Filtration
- Eliminate Bandwidth Overages
- Web Exploit Defense
- Advanced HTTP Filtration
- Anycast DNS
- Spam Eliminator



DoS/DDoS attacks could cause huge financial losses, reputation damage, and customer attrition, among other things. This section deals with pen-testing methodology to identify the scope of DoS/DDoS attacks beforehand.



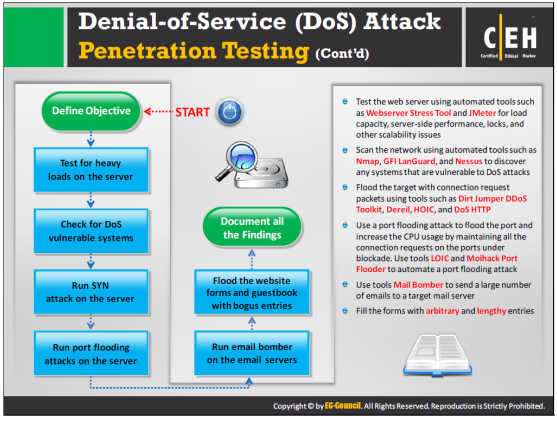
Denial-of-service attacks can compromise the computers in a network. They can disorganize an organization's functioning, depending on the nature of the attack. Organizations can lose a great deal of money while network resources are disabled. DoS attacks come in a variety of forms and target a variety of services.

Generally, in a DoS attack, the attacker sends illegitimate SYN or ping requests that overwhelm the capacity of a network, thus leaving the network unable to handle legitimate connection requests. Services running on the remote machines crash due to the specially crafted packets that are flooded over the network. In such cases, the network cannot differentiate between legitimate and illegitimate data traffic. DoS attacks can easily bring down a server. Attackers do not need to have a great deal of knowledge to conduct them, making it essential to test for DoS vulnerabilities.

Pen testers should incorporate DoS attack into pen-testing plans to determine whether a network server is susceptible to DoS attacks. DoS pen testing determines a minimum threshold for DoS attacks on a system, but the tester cannot ensure that the system is resistant to DoS attacks. The pen tester floods the target network with traffic—mimicking hundreds of people repeatedly requesting the service—to check the system stability. Thus, pen testing results help administrators determine and adopt suitable network perimeter security controls such as load balancing, IDS, IPS, Firewalls, and so on.

Launching a DoS attack can have a negative impact on the business of an organization. Therefore, prior to verifying a vulnerability to a DoS attack by actually launching it, the penetration testing team should check with the client. The result of the attack can lead to a loss

of reputation along with economic losses. A successful DoS attack can disable computers and, subsequently, an entire network. An attack launched by a moderately configured system can crash PCs that are of high value.



Discussed below are the steps involved in the DoS-attack penetration testing process:

Step 1: Define the objective

The first step in any penetration testing process is to define an objective. This helps you to plan and determine the actions that help you accomplish the goal of the test.

Step 2: Test for heavy loads on the server

To perform load testing, the penetration tester should put an artificial load on a server or application to test its stability and performance. This involves the simulation of a real-time scenario. Test a web server for load capacity, server-side performance, locks, and other scalability issues, using automated tools such as **Webserver Stress Tool** and **JMeter**.

Step 3: Check for DoS vulnerable systems

The penetration tester should scan the network to discover any systems that are vulnerable to DoS attacks, using automated tools such as **Nmap**, **GFI LanGuard**, and **Nessus**.

Step 4: Run a SYN attack on the server

A penetration tester should try to run a SYN attack on the main server by bombarding the target with connection request packets, using tools such as **Dirt Jumper DDoS Toolkit**, **Dereil**, **HOIC**, and **DoS HTTP**.

Step 5: Run port flooding attacks on the server

Port flooding sends a large number of TCP or UDP packets to a particular port, creating a denial of service on that port. The main purpose of this attack is to make the ports unusable and increase the CPU's usage to 100%. Both TCP and UPD ports are vulnerable to port flooding attacks. Use tools such as **LOIC** (Low Orbit Ion Cannon) and **Moihack Port Flooder** to automate a port flooding attack.

Step 6: Run an email bomber on the email servers

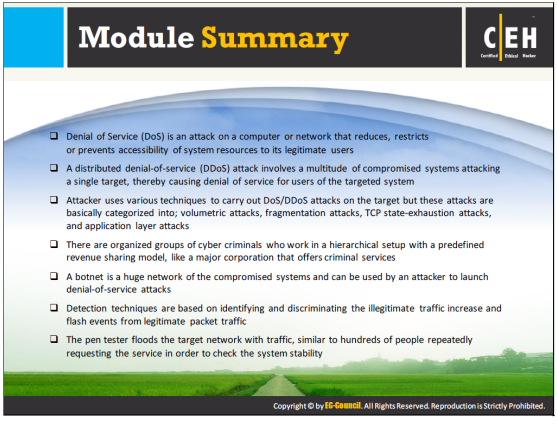
The penetration tester should send a large number of emails to test the target mail server, using tools such as **Mail Bomber**. If the server is not protected or strong enough, it will crash.

Step 7: Flood the website forms and guestbook with bogus entries

The penetration tester should fill the online website forms and guestbook with arbitrary and lengthy entries, and then submit them to check whether the data server is able to handle the load.

Step 8: Document all the findings

Finally, document all the findings at each step of the DoS pen-testing methodology for analysis and future reference.



This module ends with an overview discussion of DoS and DDoS attacks, DoS/DDoS attack techniques, botnet network, DoS/DDoS attack tools, techniques to detect DoS/DDoS attacks, countermeasures, and pen testing. In the next module, we will see how attackers, as well as ethical hackers and pen testers, perform session hijacking to steal a valid session ID.