What is a cyber attack?

An attack on an information or computer network as an “attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of anything that has value to the organization.”

A distributed-denial-of-service, or DDoS, attack is the bombardment of simultaneous data requests to a central server. The attacker generates these requests from multiple compromised systems.

In doing so, the attacker hopes to exhaust the target’s Internet bandwidth and RAM. The ultimate goal is to crash the target’s system and disrupt its business.

3 general types of DDoS attacks

Volume-based attacks

UDP flood: User Datagram Protocol (UDP) floods attack random ports on a remote server with requests called UDP packets. The host checks the ports for the appropriate applications. When no application can be found, the system responds to every request with a “destination unreachable” packet. The resulting traffic can overwhelm the service.
ICMP (ping) flood: An Internet Control Message Protocol (ICMP) flood sends ICMP echo request packets (pings) to a host. Pings are common requests used to measure the connectivity of two servers. When a ping is sent, the server quickly responds. In a ping flood, however, an attacker uses an extensive series of pings to exhaust the incoming and outgoing bandwidth of the targeted server.

Application attacks

HTTP flood: An HTTP flood is a Layer 7 application attack that uses botnets, often referred to as a “zombie army.” In this type of attack, standard GET and POST requests flood a web server or application. The server is inundated with requests and may shut down. These attacks can be particularly difficult to detect because they appear as perfectly valid traffic.
Slowloris: Named after the Asian primate, the Slowloris moves slowly. The attack sends small portions of an HTTP request to a server. These portions are sent in timed intervals, so the request does not time out, and the server waits for it to be completed. These unfinished requests exhaust bandwidth and affect the server’s ability to handle legitimate requests.

Protocol attacks

SYN flood: In a SYN flood attack, the attacker sends seemingly normal SYN requests to a server, which responds with a SYN-ACK (synchronized-acknowledgment) request. Typically, a client then sends back an ACK request, and a connection is made. In a SYN flood attack, the attacker does not respond with a final ACK. The server is left with a large number of unfinished SYN-ACK requests that burden the system.

Ping of Death: In a Ping of Death attack, the attacker tries to crash or freeze a server by sending a normal ping request that is either fragmented or oversized. The standard size of an IPv4 header is 65,535 bytes. When a larger ping is sent, the targeted server will fragment the file. Later, when the server formulates a response, the reassembly of this larger file can cause a buffer overload and crash.

Denial-of-service (DoS) and **distributed denial-of-service (DDoS)** attacks: These attacks inundate a system's resources, overwhelming them and preventing responses to service requests, and greatly reducing the system's ability to perform.

- The goal of DoS or DDoS is usually service denial or setting up a different, second attack.
- Several different types of DoS and DDoS attacks include the following:
  - **Transmission Control Protocol (TCP) synchronize (SYN) flooding** or **SYN attack**:
    - **What does a TCP SYN flooding attack target?** During a TCP session initialization handshake, the attacker takes advantage of buffer space, exploiting it to flood the target's system with connection requests.
    - **What's the result of a TCP SYN flooding attack?** The targeted system will crash or become unusable due to the overburdened system's small in-process queue.
    - **How can you prevent a TCP SYN flooding attack?**
      - First configure your firewall to halt any inbound SYN packets, then place your servers behind that firewall.
      - Boost the connect queue's size and reduce the timeout rate for open connections.

Botnets or **bots**: Botnets are comprised of a series of interconnected computers, sometimes comprised of zombie systems or just computers infected with malware.

- **What does a botnet attack target?** These bots are under the attacker's control and are used to perform an attack against the targeted computer system, network, network device, website or similar IT environment.
- **What's the result of a botnet attack?** The attacker uses the bots to bombard the victim's system, overwhelming its bandwidth and processing capabilities. Disruption is usually the botnet attacker's goal, often preventing normal working operations or otherwise degrading the victim's system's overall service.
- **What's scary about botnet attacks?**
  - Botnet attacks are notoriously hard to trace due to the many different geographic locations that the different bots can have.
  - There's no limit to how many systems these attackers can control. One attacker's bots can number in the hundreds, thousands, or even millions.

- **How can you prevent a botnet attack?** Different types of filtering offer countermeasures against botnet attacks. Techopedia offers the following examples:
    - RFC3704 filtering denies traffic from spoofed addresses and helps ensure that traffic is traceable back to its correct source network.
    - Black hole filtering drops undesirable traffic before it enters a protected network. As soon as a DDoS attack is detected, the Border Gateway Protocol (BGP) host sends routing updates to internet service provider (ISP) routers. This process helps the ISP routers direct all web traffic destined for a victim's servers onto a null0 interface.

An **intrusion detection system** (**IDS**) is a device or software application that monitors a network or systems for malicious activity or policy violations. Any intrusion activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system combines outputs from multiple sources and uses alarm filtering techniques to distinguish malicious activity from false alarms.

[illegible]

- IDS can be classified into three main categories host-based, network-based, and hybrid-based.

i. *Host-based* IDS monitors a single system. In most cases, the IDS software runs on the host. It looks for logs and activities occurring on the system and tries to find anomalies.
ii. *Network-based* IDS system monitors a network segment in which IDS is sampling all the packets that pass through a specific point on the network. The network interface card listens to all the packets.
iii. *Hybrid-based* IDS, both host-based and network-based IDSs, can be used at the same time.

IDS

i. Misuse or signature-based detection model: The IDS has knowledge of suspicious behavior in which it looks for a recognized attack in its database by comparing the current activities with a signature attack in which if the system discovers a pattern it will send an alarm.

ii. Anomaly detection model: The IDS has knowledge of normal behavior, it looks for usage anomalies by sampling normal activities and an alarm of abnormal behaviors. However, it might result in several false-positive alarms.

Eavesdropping

Eavesdropping is the act of secretly or stealthily listening to the private conversation or communications of others without their consent in order to gather information. The practice is widely regarded as unethical, and in many jurisdictions is illegal. Network protocols that use cleartext transmission to send a password, such as the File Transfer Protocol (FTP), are most susceptible to eavesdropping. Most networks rely on shared media, in which any computer connected to the network cable can potentially listen in on all network traffic that goes across the network cable. Unless this network traffic is encrypted, anyone with sinister intentions can record the network packets that are exchanged between other computers. This allows anyone with physical access to a network segment to eavesdrop on the network traffic that flows across this segment. This may include users inside your organization or someone who can plug a computer into a network connection that's located in unattended locations, such as a lobby or an unoccupied conference room.

Snooping

Snooping, in a security context, is unauthorized access to another person's or company's data. The practice is similar to eavesdropping but is not necessarily limited to gaining access to data during its transmission. Snooping can include casual observance of an e-mail that appears on another's computer screen or watching what someone else is typing. More sophisticated snooping uses software programs to remotely monitor activity on a computer or network device.

Although snooping has a negative connotation in general, in computer technology snooping can refer to any program or utility that performs a monitoring function. For example, a snoop server is used to capture network traffic for analysis, and the snooping protocol monitors information on a computer bus to ensure efficient processing.

Keystroke loggers (also known as *keyloggers*) record the keystrokes typed on a computer's keyboard. Keystroke loggers record passwords and capture the information before encryption is used on the password. There are two types of keystroke loggers: hardware and software.

Some advantages of hardware keystroke loggers are that they are completely undetectable by software, can record all keystrokes, and can record keystrokes before the operating system is loaded (such as the Basic Input Output System [BIOS] boot password). One disadvantage is that the attacker has to return to retrieve the hardware keystroke logger. An attacker can also be an insider (e.g., co-workers, a disgruntled employee, or someone on the cleaning crew).
Software keystroke loggers have many advantages over their hardware counterparts. They can be installed through social engineering attacks, can discern which program is accepting the keyboard input from the user, and can categorize the keystrokes for the attacker. They can send the captured keystrokes to the attacker via e-mail, Internet Relay Chat (IRC), or other communication channel.

Firewalls

Firewall technology filters network traffic and blocks malicious users from attacking the network system. It prevents users from intruding into private networks. Having a firewall in the entrance to a network system requires user authentications before allowing actions performed by users. There are different types of firewall technologies that can be applied to different types of networks.

A firewall is a **network security** device that monitors incoming and outgoing network traffic and permits or blocks data **packets** based on a set of security rules. Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.

Types of firewalls

Firewalls can either be software or hardware, though it’s best to have both. A software firewall is a program installed on each computer and regulates traffic through port numbers and applications, while a physical firewall is a piece of equipment installed between your network and gateway.

Packet-filtering firewalls, the most common type of firewall, examine packets and prohibit them from passing through if they don’t match an established security rule set. This type of firewall checks the packet’s source and destination IP addresses. If packets match those of an “allowed” rule on the firewall, then it is trusted to enter the network.

Packet-filtering firewalls are divided into two categories: stateful and stateless. Stateless firewalls examine packets independently of one another and lack context, making them easy targets for hackers. In contrast, stateful firewalls remember information about previously passed packets and are considered much more secure.

While packet-filtering firewalls can be effective, they ultimately provide very basic protection and can be very limited—for example, they can't determine if the contents of the request that's being sent will adversely affect the application it's reaching. If a malicious request that was allowed from a trusted source address would result in, say, the deletion of a database, the firewall would have no way of knowing that. Next-generation firewalls and proxy firewalls are more equipped to detect such threats.

Next-generation firewalls (NGFW) combine traditional firewall technology with additional functionality, such as encrypted traffic inspection, intrusion prevention systems, anti-virus, and more. Most notably, it includes deep packet inspection (DPI). While basic firewalls only look at packet headers, deep packet inspection examines the data within the packet itself, enabling users to more effectively identify, categorize, or stop packets with malicious data. Next Generation Firewalls inspect packets at the application level of the TCP/IP stack and are able to identify applications such as Skype, or Facebook and enforce security policy based upon the type of application.

Proxy firewalls filter network traffic at the application level. Unlike basic firewalls, the proxy acts an intermediary between two end systems. The client must send a request to the firewall, where it is then evaluated against a set of security rules and then permitted or blocked. Most notably, proxy firewalls monitor traffic for layer 7 protocols such as HTTP and FTP, and use both stateful and deep packet inspection to detect malicious traffic.

Network address translation (NAT) firewalls allow multiple devices with independent network addresses to connect to the internet using a single IP address, keeping individual IP addresses hidden. As a result, attackers scanning a network for IP addresses can't capture specific details, providing greater security against attacks. NAT firewalls are similar to proxy firewalls in that they act as an intermediary between a group of computers and outside traffic.

Stateful multilayer inspection (SMLI) firewalls filter packets at the network, transport, and application layers, comparing them against known trusted packets. Like NGFW firewalls, SMLI also examine the entire packet and only allow them to pass if they pass each layer individually. These firewalls examine packets to determine the state of the communication (thus the name) to ensure all initiated communication is only taking place with trusted sources.

What is an Intrusion Prevention System – IPS

In short, an Intrusion Prevention System (IPS), also known as intrusion detection prevention system (IDPS), is a technology that keeps an eye on a network for any malicious activities attempting to exploit a known vulnerability. An intrusion prevention system (IPS) is a form of network security that works to detect and prevent identified threats. Intrusion prevention systems continuously monitor your network, looking for possible malicious incidents and capturing information about them. The IPS reports these events to system administrators and takes preventative action, such as closing access points and configuring firewalls to prevent future attacks. IPS solutions can also be used to identify issues with corporate security policies, deterring employees and network guests from violating the rules these policies contain.

Why should Intrusion Prevention Systems be used?

IPS technologies can detect or prevent network security attacks such as brute force attacks, Denial of Service (DoS) attacks and vulnerability exploits. A vulnerability is a weakness in a software system and an exploit is an attack that leverages that vulnerability to gain control of a system. When an exploit is announced, there is often a window of opportunity for attackers to exploit that vulnerability before the security patch is applied. An Intrusion Prevention System can be used in these cases to quickly block these attacks.

Because IPS technologies watch packet flows, they can also be used to enforce the use of secure protocols and deny the use of insecure protocols such as earlier versions of SSL or protocols using weak ciphers.

How do Intrusion Prevention Systems work?

IPS technologies have access to packets where they are deployed, either as Network intrusion detection systems (NIDS), or as Host intrusion detection systems (HIDS). Network IPS has a larger view of the entire network and can either deployed inline in the network or offline to the network as a passive sensor that receives packets from a network TAP or SPAN port.

The detection method employed may be signature or anomaly-based. Predefined signatures are patterns of well-known network attacks. The IPS compares packet flows with the signature to see if there is a pattern match. Anomaly-based intrusion detection systems uses heuristics to identify threats, for instance comparing a sample of traffic against a known baseline.

What’s the difference between IDS and IPS?

Early implementations of the technology were deployed in detect mode on dedicated security appliances. As the technology has matured and moved into integrated Next Generation Firewall or UTM devices, the default action is set to prevent the malicious traffic.

In some cases, the decision to detect and accept or prevent the traffic is based upon confidence in the specific IPS protection. When there is lower confidence in an IPS protection, then there is a higher likelihood of false positives. A false positive is when the IDS identifies an activity as an attack but the activity is acceptable behavior. For this reason, many IPS technologies also have the ability to capture packet sequences from the attack event. These can then be analyzed to determine if there was an actual threat and to further improve the IPS protection.