Chapter 10: Denial-of-Service (DoS)

Introduction

A Denial-of-Service (DoS) attack attempts to shut down a machine or network, making it unreachable to its intended users. DoS attacks achieve this by providing the victim with excessive traffic or information that causes a system breakdown. The attack denies the service or resource that legitimate users (such as employees, members, or account holders) expected. DoS attacks generally target the web servers of well-known corporations, including media, financial, and commercial companies, as well as governmental and commercial organizations. Although they seldom lead to the loss or theft of important data or other assets, they can still be very time-consuming and money-consuming for the victims.

In this chapter, you will explore:

- Fundamental concept of Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks
- Role of botnets in executing large-scale DDoS attacks
- Case study of a real-world DDoS attack
- Various techniques used in DoS and DDoS attacks
- Countermeasures to defend the system against DoS and DDoS attacks

DoS/DDoS Concepts

DoS Attack

A Denial-of-Service (DoS) attack on a system or network results in the Denial-of-Service or services, reduction in functions and operation of that system, or prevention of legitimate users accessing the resources. In short, a DoS attack on a service or network makes it unavailable for legitimate users. The technique for performing a DoS attack is to generate huge traffic to the target system requesting a specific service. This unexpected traffic overloads the system's capacity and either results in a system crash or unavailability.

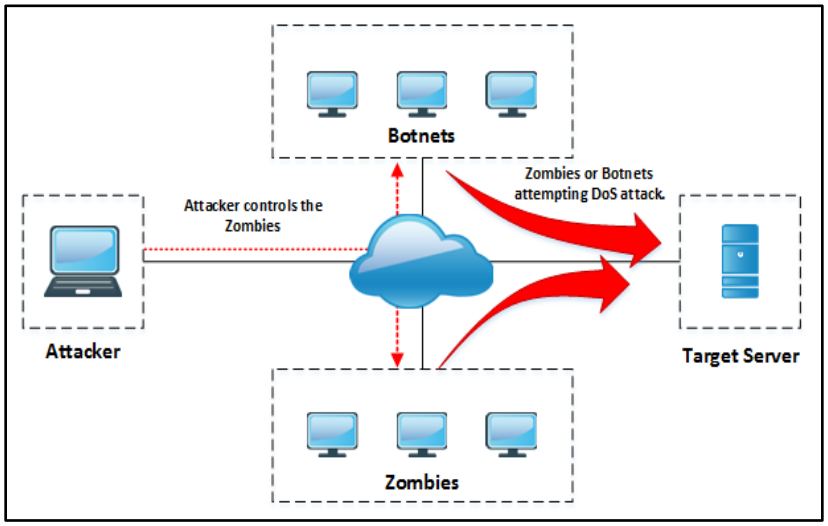

Figure 10-01: Denial-of-Service Attack

Common symptoms of DoS attacks are:

- Slow performance
- Increase in spam emails
- Unavailability of a resource
- Loss of access to a website
- Disconnection of a wireless or wired internet connection
- Denial of access to any internet service

Distributed Denial-of-Service (DDoS)

DDoS is similar to DoS, in which an attacker generates fake traffic. In a Distributed DoS attack, multiple compromised systems are involved in attacking a target to cause a Denial-of-Service. Botnets are used for carrying out a DDoS attack.

EXAM TIP: DoS disrupts services by overwhelming systems with traffic, while DDoS amplifies this using distributed botnets. Focus on the distinction between volumetric, protocol, and application-layer attacks.

How Distributed Denial-of-Service Attacks Work

Usually, establishing a connection consists of a few steps: a user sends a request to a server to authenticate it. The server returns with authentication approval, and the user acknowledges that approval. Then, the connection is established and allowed onto the server.

An attacker sends several authentication requests to the server during a denial-of-service attack. These requests have fake return addresses, meaning the server cannot find a user to send authentication approval. The server typically waits more than a minute before closing the session. By continuously sending requests, the attacker causes several open connections on the server, resulting in the Denial-of-Service.

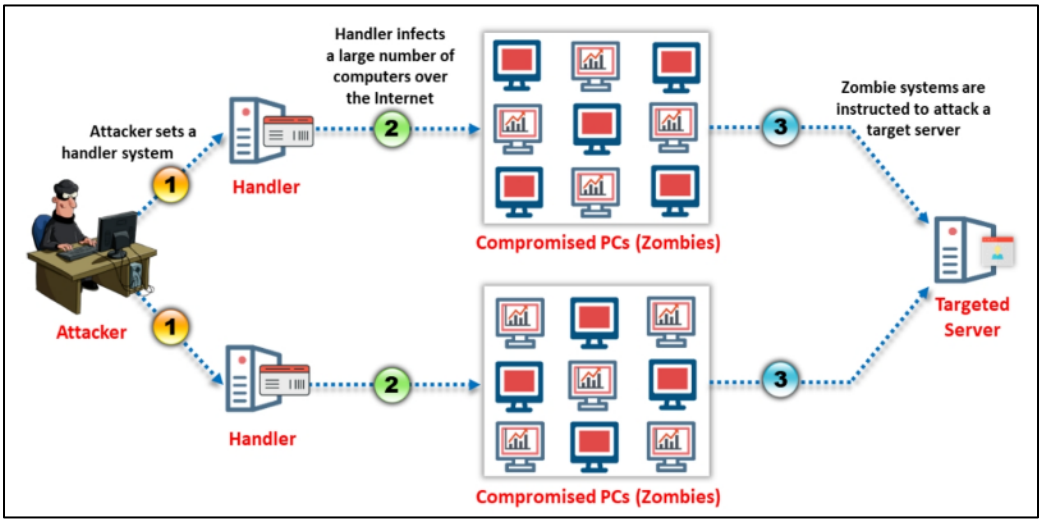

Figure 10-02: Schematic of a DDoS Attack

Botnets

Botnets are used for continuously performing a task. These malicious botnets gain access to a system using malicious scripts and codes. This alerts the master computer when the botnets start controlling the system. Through this master computer, an attacker can control the system and issue requests to attempt a DoS attack.

Organized Cyber Crime: Organizational Structure

Organized Crime Syndicates

Cyber criminals operated independently in the past; however, there has been a notable shift towards collaboration within organized groups. These individuals are increasingly linked to organized crime syndicates, leveraging the advanced methodologies of these entities to conduct illegal activities, primarily for financial gain. Within this framework, cyber criminals function in a structured hierarchy with a defined revenue-sharing arrangement, resembling a corporate model that provides criminal services. These organized groups are responsible for creating and renting botnets, as well as offering a range of services that include malware development, bank account hacking, and executing large-scale DoS attacks for a fee. For instance, a crime syndicate may perform a DDoS attack on a financial institution to distract its security personnel while simultaneously draining funds from compromised accounts. The escalating participation of organized crime syndicates in politically driven cyber warfare and hacktivism raises significant concerns for national security agencies. The landscape of cybercrime is intricate, featuring a diverse array of participants, with compensation based on the specific tasks performed or the roles held within the organization. At the apex of the cybercrime hierarchy is the leader, who functions as an entrepreneur without directly engaging in criminal acts. Directly beneath the leader is the "underboss," responsible for establishing a command and control server and maintaining a database of crimeware toolkits to facilitate attacks and supply Trojans. Below the underboss are several "campaign managers," each overseeing their networks for executing attacks and acquiring data. Ultimately, resellers are tasked with selling the stolen information.

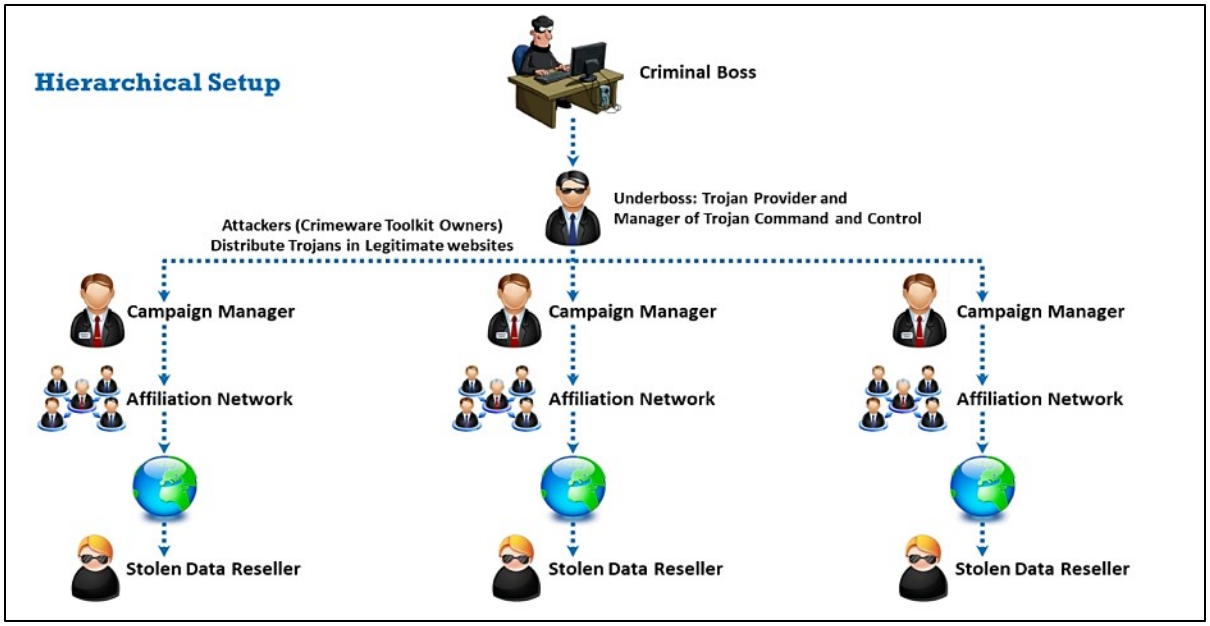

Figure 10-03: Hierarchical Setup of a Cybercrime

Botnets

Bots serve various functions, including benign data collection and data mining activities, such as web spidering, as well as orchestrating Denial-of-Service (DoS) attacks. The primary function of a bot is data collection. There are several categories of bots, including Internet bots, IRC bots, and chatterbots. Notable examples of IRC bots include Cardinal, Sopel, Eggdrop, and EnergyMech. A botnet, which is a combination of the terms "robot" and "network," refers to a collection of computers that bots have compromised. While botnets can be utilized for beneficial purposes, they are often associated with malicious activities. As a tool for cybercriminals, a botnet consists of a vast network of infected systems.

Even a relatively small botnet, comprising 1,000 bots, can possess a combined bandwidth that exceeds that of most corporate networks. The emergence of botnets has significantly contributed to the rise of cybercrime. They serve as the backbone of cybercriminal operations, connecting various elements of the cybercrime ecosystem. Cybercriminal service providers are integral to this network, offering services such as the development of malicious code, bulletproof hosting, browser exploit creation, and encryption and packing. Malicious code is the primary instrument employed by criminal organizations to execute cybercrimes. Botnet operators can command both bots and other malicious software, including Trojans, viruses, worms, keyloggers, and specially designed applications, to target remote computers through networks. Malware services are often advertised on public platforms or restricted online resources. Botnets act as agents that intruders can deploy to server systems to carry out illegal activities. They execute concealed programs that help identify system vulnerabilities.

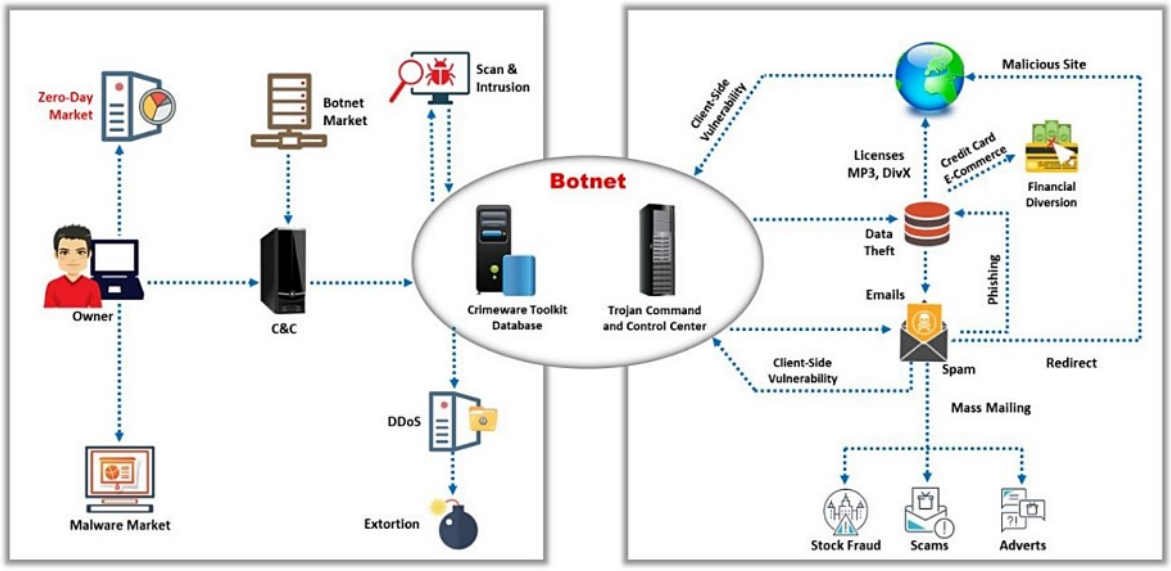

Figure 10-04: Botnet Ecosystem

EXAM TIP: Botnets are networks of compromised devices used to launch large-scale attacks. Defenses against botnets include IP reputation filtering to block known malicious IPs, black-hole routing to drop malicious traffic, and ISP-level protections that work with internet providers to filter traffic before it reaches the target network.

Attackers can leverage botnets to conduct various tasks, including:

- **DDoS attacks:** Botnets can initiate Distributed Denial-of-Service (DDoS) attacks, which deplete the bandwidth of the targeted computers. Additionally, botnets can overwhelm a system, consuming critical host system resources and disrupting network connectivity.
- **Spamming:** Attackers utilize SOCKS proxies to facilitate spamming activities. They gather email addresses from websites and other sources for this purpose.
- **Traffic Sniffing:** A packet sniffer can monitor the data traffic flowing into a compromised device, enabling attackers to gather sensitive information such as credit card details and passwords. This tool also allows for the theft of data from one botnet to be exploited against another.
- **Keylogging:** This technique involves recording keystrokes on a keyboard, thereby capturing sensitive information like system passwords. Attackers employ keyloggers to obtain login credentials for various services, including PayPal.
- **Disseminating New Malware:** Botnets can be utilized to propagate new malicious software.
- **Installing Advertising Add-ons:** Botnets can engage in "click fraud" by automating clicks on advertisements.

- **Abuse of Google AdSense:** Certain companies allow the display of Google AdSense ads on their platforms for financial gain. Botnets can automate clicks on these ads, artificially inflating the click count.
- **Attacks on IRC Networks:** Known as clone attacks, these are akin to DDoS attacks. A master agent directs each bot to connect to numerous clones within an IRC network, potentially overwhelming it.
- **Manipulating Online Polls and Games:** Each botnet possesses a distinct address, which enables it to influence online polls and gaming outcomes.
- **Mass Identity Theft:** Botnets can dispatch a significant volume of emails while masquerading as reputable entities, such as eBay, facilitating the theft of personal information for identity fraud.
- **Credential Stuffing:** With access to a multitude of compromised devices, attackers can automate the process of credential stuffing.
- **Cryptocurrency mining:** Malicious actors can deploy cryptocurrency mining software on compromised devices within a botnet, leveraging their computational resources to mine cryptocurrency without the owners' knowledge or consent.

Figure 10-05 depicts the process by which an attacker initiates a botnet-based Denial-of-Service (DoS) attack against a targeted server. Initially, the attacker establishes a Command and Control (C&C) center for the botnet, after which they infect a single machine (referred to as a bot) and gain control over it. This compromised bot is then utilized to infiltrate and compromise additional vulnerable systems within the network, thereby forming a botnet. The infected machines, commonly referred to as zombies, connect to the C&C center and await further instructions. Subsequently, the attacker transmits harmful commands to the bots via the C&C center. Ultimately, in accordance with the attacker's directives, the bots execute a DoS attack on the designated server, rendering its services inaccessible to legitimate users within the network.

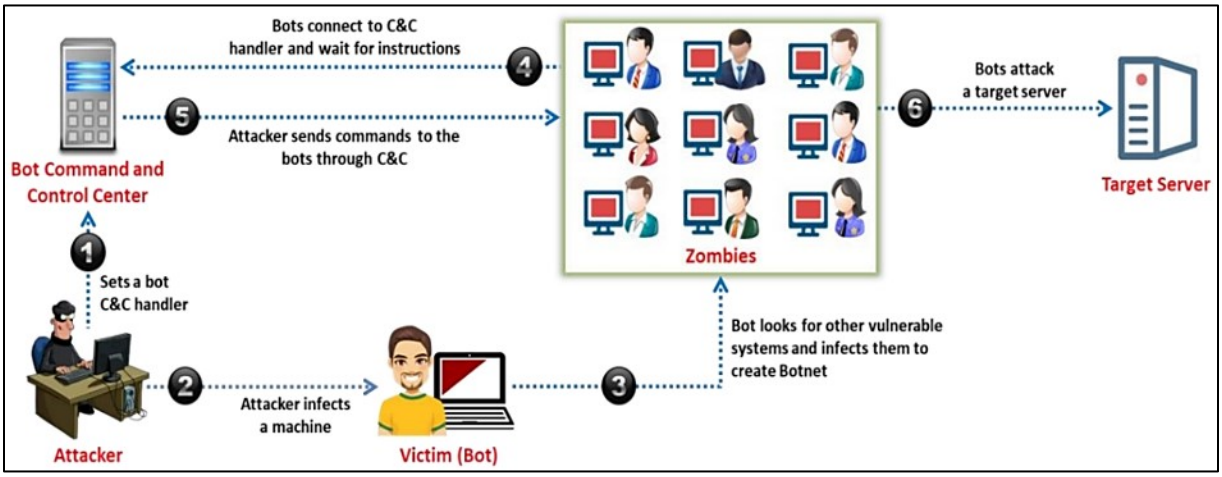

Figure 10-05: Botnet Based DDoS Attack

Typical Botnet Setup

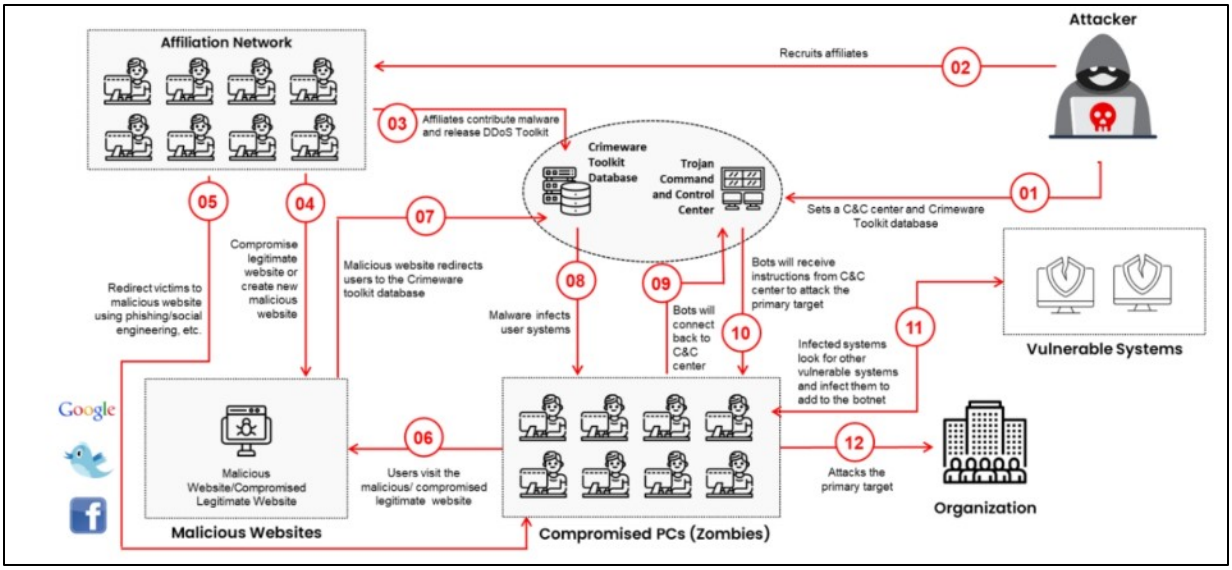

Figure 10-06: Typical Botnet Setup

Scanning Techniques for Identifying Vulnerable Systems

The following are scanning techniques employed by attackers to identify vulnerable systems within a network:

Random Scanning

This method involves an infected machine, either the attacker's device or a compromised system, randomly probing IP addresses within the target network's range to assess their vulnerabilities. Upon identifying a vulnerable system, the attacker exploits it and attempts to infect it by deploying the same malicious code present on the initial machine. This approach generates considerable network traffic, as multiple compromised machines may simultaneously probe the same IP addresses. Initially, malware spreads rapidly, but the rate of propagation diminishes as the pool of new IP addresses becomes limited over time.

Hit-list Scanning

In this approach, an attacker first compiles a list of potentially vulnerable systems and subsequently assembles a network of compromised machines. The attacker then scans this list to locate a vulnerable system. Once identified, the attacker installs malicious code on it and divides the list into two halves. The attacker continues scanning one half while the newly compromised machine scans the other half. This iterative process leads to an exponential increase in the number of compromised systems, ensuring that malicious code is installed on all potentially vulnerable machines within the hit list in a relatively short timeframe.

Topological Scanning

This technique leverages information obtained from an infected machine to discover new vulnerable systems. An infected host examines the hard drive of the target machine for URLs it wishes to infect. It then compiles a shortlist of URLs and assesses their vulnerabilities. This method

produces accurate results and exhibits performance comparable to that of the hit-list scanning technique.

Local Subnet Scanning

In this technique, an infected machine seeks out new vulnerable systems within its local network, even those protected by a firewall, by utilizing information concealed within local addresses. Attackers frequently employ this method in various scenarios.

Permutation Scanning

This method involves attackers utilizing a shared pseudorandom permutation list of IP addresses belonging to all machines. The list is generated through a 32-bit block cipher combined with a predetermined key. In instances where a compromised host is detected during either hit-list scanning or local subnet scanning, the scanning process resumes from the point immediately following the compromised host to seek out additional targets. Conversely, if a compromised host is identified during permutation scanning, the scanning process restarts from a randomly selected point. Should an already infected machine be encountered, the scanning will again restart from a new random position within the permutation list. The scanning procedure concludes when the compromised host repeatedly encounters a specified number of already infected machines without discovering new targets. Following this, a new permutation key is created to commence a fresh scanning phase.

Scanning Vulnerable Machines

There are several techniques used for scanning vulnerable machines, including Random, Hit-list, Topological, Subnet, and Permutation Scanning. A brief description of these scanning methods is given below:

Scanning Method	Description
Random Scanning Technique	An infected machine probes IP addresses randomly from an IP pool and scans for vulnerabilities. If it finds a vulnerable machine, it breaks and infects it with malicious script. The random scanning technique spreads the infection very quickly; it can compromise a large number of hosts
Hit-List Scanning Technique	The attacker first collects information about a large number of potentially vulnerable machines to create a Hit-list. An attacker finds a machine with vulnerabilities and infects it using this technique. Once a machine is infected, the list is divided into two by assigning half to the newly compromised system. The scanning process in the hit-list scanning runs simultaneously. This technique is used to ensure the spread and installation of malicious code in a short period
Topological Scanning Technique	Topological Scanning gathers information such as URLs from an infected system to find another vulnerable target. The initially compromised machine searches a URL from the disk and scans for vulnerability. As these URLs are valid (taken from the disk), the accuracy of this technique is extremely good

Subnet Scanning Technique	This technique is used to attempt scanning behind a firewall where the compromised host is scanning for vulnerable targets in its own local network. This technique is used for forming an army of zombies in a short span of time
Permutation Scanning Technique	Permutation scanning uses a pseudorandom permutation. In this technique, infected machines share the pseudorandom permutation of IP addresses. If scanning detects an infected system by either hit-list scanning or any other method, it continues scanning from the next IP in the list. If scanning detects an already infected system by permutation list, it starts scanning from a random point in the permutation list

Table 10-01: Scanning Methods for Finding Vulnerable Machines

How Does Malicious Code Spread?

Below are three methods employed by attackers to disseminate malicious code and establish attack networks:

Central Source Propagation

In this method, the attacker deploys an attack toolkit on a central server, from which a copy is sent to a newly identified vulnerable system. Upon discovering a susceptible machine, the attacker directs the central server to transmit a copy of the attack toolkit to the newly compromised device, where the attack tools are automatically installed through a scripting mechanism. This process initiates a new cycle of attacks as the newly infected machine seeks out additional vulnerable systems to repeat the installation of the attack toolkit. Typically, this method utilizes protocols such as HTTP, FTP, and RPC.

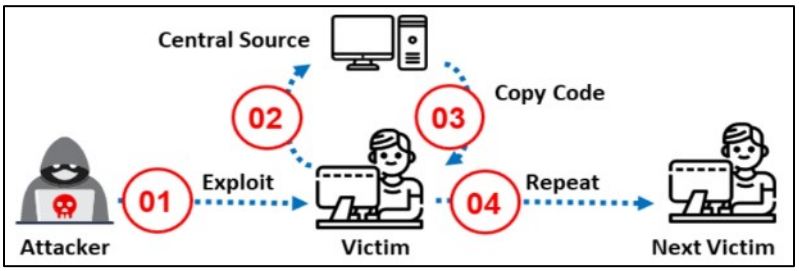

Figure 10-07: Central Source Propagation

Back-chaining Propagation

In this approach, the attacker maintains an attack toolkit on their system, which is then transferred to a newly identified vulnerable system. The attack tools on the attacking machine employ specific techniques to accept connections from the compromised system, subsequently transferring a file containing the attack tools. This back-channel file transfer is facilitated by simple port listeners or fully installed web servers on the intruder's machine, both utilizing the Trivial File Transfer Protocol (TFTP).

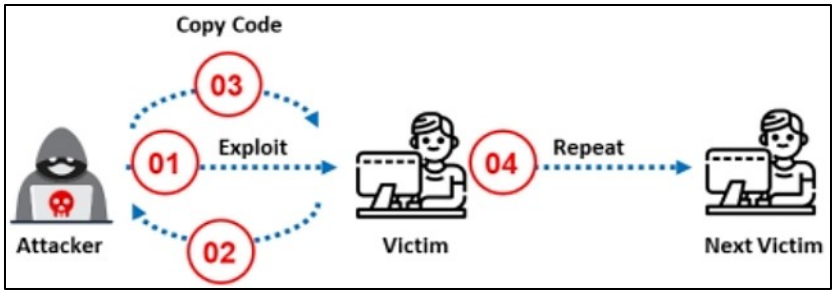

Figure 10-08: Back Chaining Propagation

Autonomous Propagation

In contrast to the previously mentioned methods, where an external file source delivers the attack toolkit, autonomous propagation involves the attacking host directly transferring the attack toolkit to a newly discovered vulnerable system at the moment it gains access to that system.

Figure 10-09: Autonomous Propagation

Botnet Trojan

- Blackshades NET
- Cythosia Botnet and Andromeda Bot
- PlugBot

DDoS Case Study

DDoS attacks represent a sophisticated and intricate form of assault that builds upon traditional DoS attacks, utilizing multiple distributed sources. In such an attack, a significant number of compromised computers, often referred to as "zombies," disrupt or halt network services. This section provides an analysis of a DDoS attack.

DDoS Attack

In a DDoS attack, perpetrators leverage a collection of compromised systems, commonly known as bots or zombies, which are typically infected with Trojan malware, to execute a DoS attack against a targeted system or network resource.

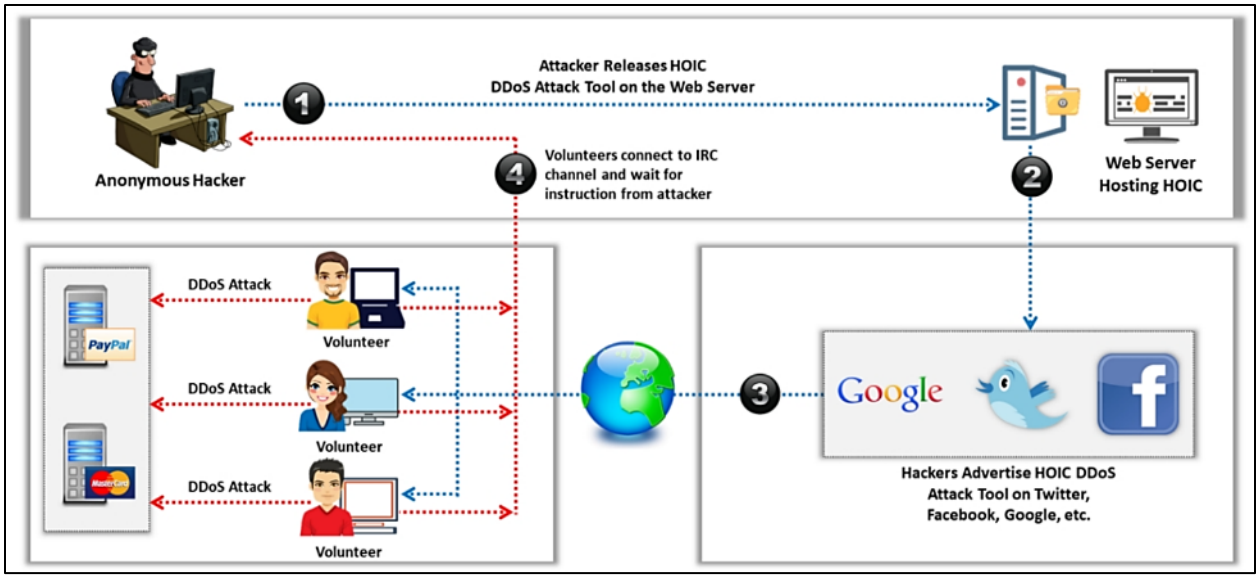

Figure 10-10: DDoS Attack Scenario

As shown in Figure 10-10, an anonymous hacker deploys a High Orbit Ion Cannon (HOIC) DDoS attack tool on either a personal web server or a compromised server. The hacker promotes the HOIC tool through social media platforms and search engines, such as Twitter, Facebook, and Google, accompanied by a malicious download link.

Individuals interested in conducting the DDoS attack may download the HOIC tool by clicking on the link provided by the hacker. These individuals are referred to as "volunteers." All volunteers connect through an IRC channel to the anonymous hacker, awaiting further instructions. The hacker directs the volunteers to inundate the target web server (for instance, PayPal, MasterCard, or PAYBACK) with a barrage of requests. Upon receiving these instructions, the volunteers execute the commands, resulting in the target server becoming overwhelmed and unresponsive to legitimate user requests.

Hackers Promote Download Links for Botnets

Hackers disseminate advertisements for botnets across various platforms, including blogs, search engines, social media, and emails, often featuring download links. They may also employ deceptive updates and security alerts to mislead victims into downloading the malware. The objective of this strategy is to propagate the botnet and expand the attack network's size. This method of attack is notably rapid and effective. Figures 10-11 illustrate examples of advertisements hosted by hackers on the Internet for downloading botnets.

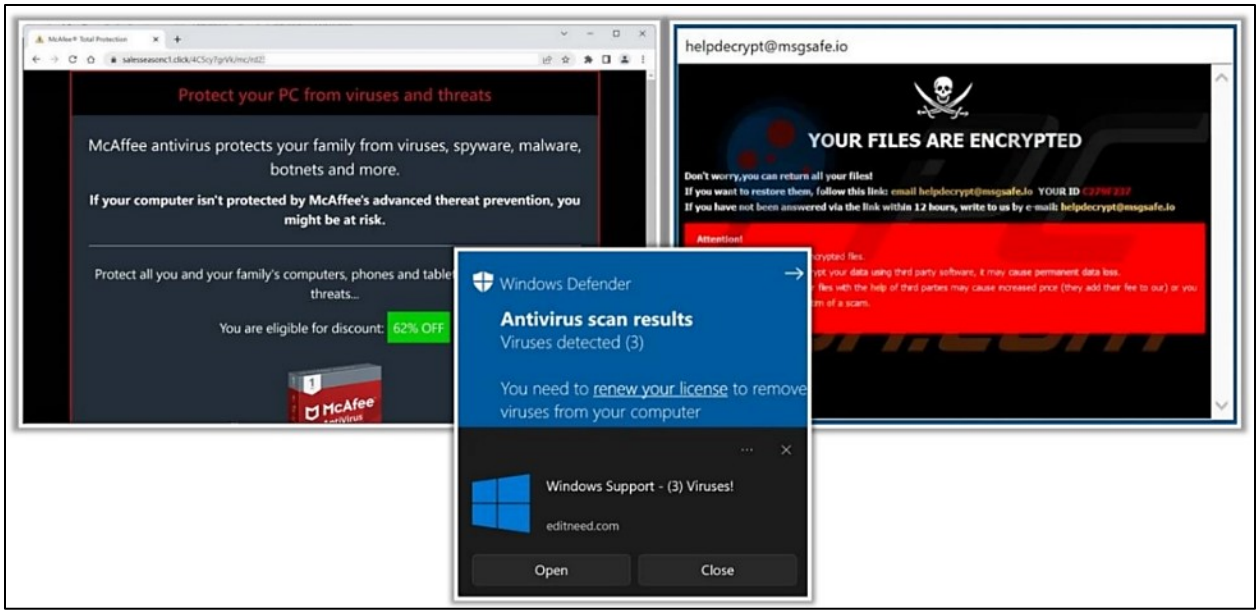

Figure 10-11: Advertisements with Links to Download Botnets

Use of Mobile Devices as Botnets for Executing DDoS Attacks

Android devices are inherently susceptible to a range of malware, including Trojans, bots, and Remote Access Trojans (RATs), which are frequently encountered in third-party application stores. These unprotected Android devices have become prime targets for cybercriminals seeking to expand their botnet networks due to their significant vulnerability to malicious software. Instances of infection methods include harmful Android applications available on the Google Play Store and those delivered through drive-by downloads. Attackers typically attach a malicious server to the Android application package (APK) file, encrypt it, and eliminate unnecessary features and permissions prior to distributing the compromised package through third-party app stores like Google Play Store. Once victims are deceived into downloading and installing these applications, their devices are commandeered by the attackers and incorporated into the attackers' mobile botnet, enabling the execution of harmful activities such as DDoS attacks and web injections.

DDoS Case Study: HTTP/2 'Rapid Reset' Attack on Google Cloud

The Google DDoS response team has issued a warning regarding the significant rise in the scale of DDoS attacks. In September 2023, the team reported successfully mitigating a formidable DDoS attack that reached 398 million requests per second (rps), a staggering 7.5 times greater than the prior attack, which peaked at 46 rps. This particular attack used innovative HTTP/2 "Rapid Reset" methods designed to disrupt websites, Internet services, and infrastructure providers.

Attack Timeline

The DDoS attack was documented in late August and continued until the conclusion of September 2023. This HTTP/2 "Rapid Reset" DDoS attack aimed to disrupt major infrastructure providers, including Google services, Google Cloud infrastructure, and their clientele, for 2-3 minutes at its peak. Despite its brief nature, the targeted services encountered an unforeseen influx of TCP packets with RST (Reset) flags intended to inundate and reset the target server.

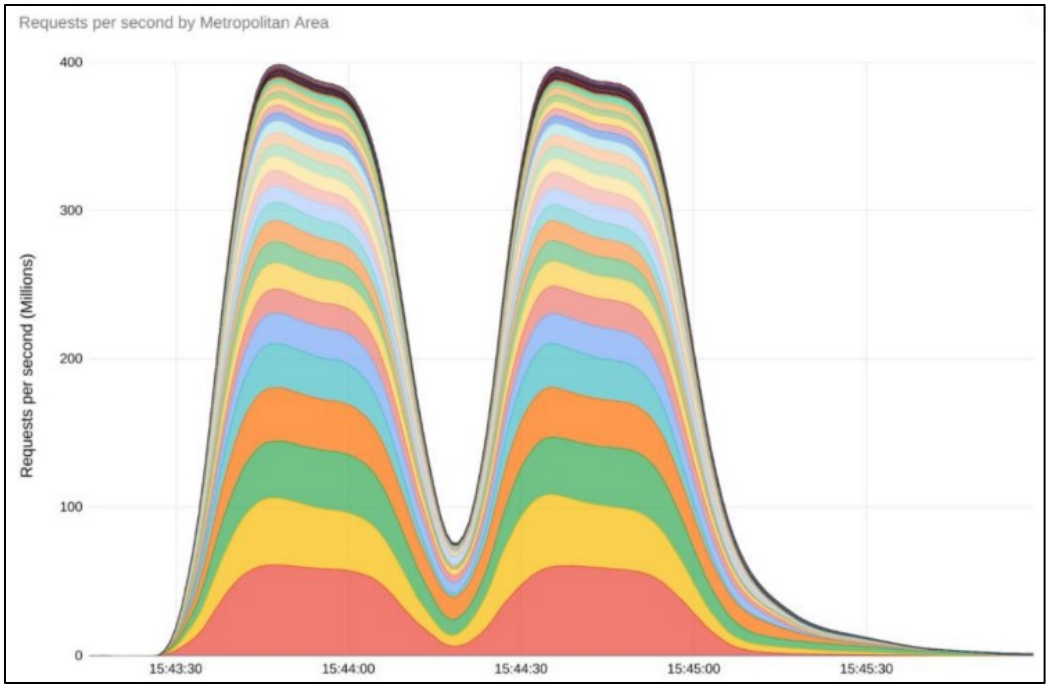

Figure 10-12: DDoS Attack Where It Peaked At 398 Million rps

Nevertheless, Google's DDoS mitigation infrastructure was instrumental in maintaining the functionality of their services. Google, in collaboration with its clients, industry partners, and the wider online community, took proactive measures to lead a joint effort to counteract the attack.

Attack Mechanism

The attack was launched utilizing an innovative "Rapid Reset" technique that capitalizes on stream multiplexing, a characteristic of the widely utilized HTTP/2 protocol. The capability of HTTP/2 to manage up to 100 concurrent streams through a single TCP connection presented a notable vulnerability. Attackers exploited this weakness by initiating a continuous series of stream requests, all of which were reset streams, resulting in considerable disruption.

Google's Response

The response team at Google claims that they effectively mitigated the attack on the perimeter of their network by leveraging their significant investment in edge capacity. This proactive approach ensured that both their services and those of their clients remained largely unaffected. As the team gained a deeper understanding of the attack techniques utilized, they formulated a series of countermeasures and enhanced their proxies and defense systems to neutralize the threat effectively. The same robust hardware and software infrastructure employed for Google's own Internet-facing services was made available to cloud customers utilizing Google Cloud's Application Load Balancer and Cloud Armor. Shortly after detecting the initial instances of the attack, Google swiftly implemented additional mitigation strategies and initiated a collaborative response with other cloud providers and software maintainers using the HTTP/2 protocol stack. Real-time threat intelligence and mitigation strategies were shared immediately to prevent significant disruption. This cross-industry collaboration led to the creation of patches and other mitigation techniques

adopted by numerous major infrastructure providers. It also enabled coordinated, responsible disclosure of the new attack methodologies and their potential effects on various widely used open-source and commercial proxies, application servers, and load balancers. The collective vulnerability to this attack was designated CVE-2023-44487 and classified as a high-severity vulnerability, receiving a CVSS score of 7.5 out of 10.

DoS/DDoS Attack Tools

Pandora DDoS Bot Toolkit

The Pandora DDoS Toolkit was developed by a Russian called Sokol, who also developed the Dirt Jumper Toolkit. The Pandora DDoS Toolkit can generate five types of attacks, including infrastructure and application-layer attacks, namely:

1. HTTP Min
2. HTTP Download
3. HTTP Combo
4. Socket Connect
5. Max Flood

Other DDoS Attack Tools

- Derail
- HOIC (High Orbit Ion Cannon)
- DoS HTTP
- BanglaDos
- R.U.D.Y(R-U-Dead-Yet)

DoS and DDoS Attack Tools for Mobile

- AnDOSid
- Low Orbit Ion Cannon (LOIC)

DoS/DDoS Attack Techniques

Attackers use multiple methods to execute DoS and DDoS attacks against specific computers or networks. This section outlines the fundamental classifications of DoS/DDoS attack vectors, the different techniques utilized in these attacks, and the various tools available for conducting DoS and DDoS attacks aimed at compromising one or more network systems, thereby depleting their computational resources or making them inaccessible to legitimate users.

Basic Categories of DoS/DDoS Attack Vectors

DDoS attacks primarily focus on depleting network bandwidth by overwhelming network, application, or service resources, thereby hindering legitimate users from accessing system or network functionalities. Generally, the vectors for DoS/DDoS attacks can be classified as follows:

Volumetric Attacks

These types of attacks aim to saturate the bandwidth either within the targeted network/service or between the targeted network/service and the broader Internet, resulting in traffic congestion that obstructs access for legitimate users. The intensity of the attack is quantified in bits per second

(bps). Volumetric DDoS attacks typically exploit protocols such as the Network Time Protocol (NTP), Domain Name System (DNS), and Simple Service Discovery Protocol (SSDP), which are stateless and lack inherent congestion management capabilities. The generation of a substantial volume of packets can lead to the complete consumption of the network's bandwidth. A single machine is insufficient to generate enough requests to overwhelm network infrastructure. Therefore, in DDoS attacks, the perpetrator employs multiple computers to inundate a target. In this scenario, the attacker can manage all the machines and direct them to send traffic to the intended system. DDoS attacks inundate a network, resulting in a significant alteration in network traffic that can incapacitate network devices such as switches and routers. Attackers leverage the computational power of numerous geographically dispersed machines to produce massive traffic directed at the victim, which is the reason such an attack is referred to as a DDoS attack.

 **EXAM TIP:** Volumetric attacks flood the network with an overwhelming amount of traffic, often exploiting protocols like NTP, DNS, and SSDP, which are vulnerable due to poor congestion management. These attacks aim to exhaust the target's bandwidth, rendering the service unavailable.

There are two primary categories of bandwidth depletion attacks:

- A flood attack involves the use of compromised systems, often referred to as zombies, which generate substantial amounts of traffic directed at the victim's systems, thereby depleting their available bandwidth.
- An amplification attack occurs when the attacker or compromised systems send messages to a broadcast IP address, resulting in an increase in malicious traffic that further drains the bandwidth of the victim's systems.

 **EXAM TIP:** Flood attacks generate traffic directly from compromised systems, while amplification attacks use broadcast protocols to increase the volume of traffic. Examples include UDP floods and NTP amplification, where attackers leverage misconfigured servers to amplify their attack.

Attackers typically utilize botnets to execute Distributed Denial-of-Service (DDoS) attacks, overwhelming the network and consuming all available bandwidth, leaving no capacity for legitimate users. The following are examples of volumetric attack techniques:

- User Datagram Protocol (UDP) flood attack
- Internet Control Message Protocol (ICMP) flood attack
- Ping of Death (PoD) attack
- Smurf attack
- Pulse wave attack
- Zero-day attack
- Malformed IP packet flood attack
- Spoofed IP packet flood attack

- NTP amplification attack

Protocol Attacks

Attackers may obstruct access to a target by depleting resources beyond mere bandwidth, such as connection state tables. Protocol DDoS attacks aim to exhaust the resources available on the target or intermediary devices connecting the target to the Internet. These attacks utilize the connection state tables found in network infrastructure components, including load balancers, firewalls, and application servers. As a result, new connections are not permitted, as the device remains occupied, waiting for existing connections to terminate or time out. The intensity of these attacks is typically quantified in packets per second (pps) or connections per second (cps). Such attacks can potentially seize control of the state of millions of connections managed by high-capacity devices.

There are some examples of protocol attack techniques include:

- Synchronize (SYN) flood attack
- Fragmentation attack
- Spoofed session flood attack
- Acknowledgment (ACK) flood attack
- SYN-ACK flood attack
- ACK and PUSH ACK flood attack
- TCP connection flood attack
- TCP state exhaustion attack
- RST attack
- TCP SACK panic attack.

Application Layer Attacks

In these types of attacks, the perpetrator seeks to exploit weaknesses within the application layer protocol or the application itself, thereby preventing legitimate users from accessing the application. Unlike protocol or volumetric DDoS attacks, assaults on unpatched and vulnerable systems do not necessitate substantial bandwidth to be effective. In application DDoS attacks, the resources of the application layer are consumed by establishing connections and maintaining them until no additional connections can be initiated. These attacks target specific components of an application or service and can be executed effectively with just one or a few attacking machines, generating a minimal traffic volume. Moreover, such attacks are notably challenging to detect and counteract. The intensity of the attack is quantified in requests per second (rps). Application-level flood attacks can lead to the disruption of services within a particular network, affecting resources such as email and other network functionalities, or may result in the temporary suspension of applications and services. Through these attacks, adversaries exploit vulnerabilities in the programming source code, preventing the application from handling legitimate requests. Various forms of DoS attacks depend on software-related vulnerabilities, including buffer overflows. A buffer overflow attack involves sending an excessive amount of data to an application, which may either cause the application to crash or compel the data to execute on the host system. This type of attack can remotely incapacitate a vulnerable system by overwhelming it with traffic directed at an application. In some instances, attackers may also be able to execute arbitrary code on the remote

system through a buffer overflow. By inundating an application with excessive data, the attacker can overwrite the control data of the program, allowing them to execute their own code.

Through application-level flood attacks, attackers aim to achieve the following objectives:

- Overload websites with traffic from legitimate users.
- Interrupt service to a particular system or individual by, for instance, preventing a user from accessing a system by repeatedly attempting an invalid login
- To disrupt the application database connection, create fraudulent SQL queries

Application-level flood attacks can inflict considerable financial losses, service interruptions, and damage to an organization's reputation. These attacks typically occur after a connection has been established, making it challenging to identify them since the incoming traffic appears legitimate. Nevertheless, if the user recognizes the attack, they can more readily stop it and trace its origin compared to other forms of Distributed Denial-of-Service (DDoS) attacks.

The following examples illustrate various techniques employed in application layer attacks:

- Hypertext Transfer Protocol (HTTP) flood attack
- Slowloris attack
- UDP application layer flood attack
- DDoS extortion attack.

DoS/DDoS Protection Tools

AWS Shield

The AWS Shield is a DDoS protection tool that examines the traffic approaching your websites using flow monitoring. By examining the flow data, the program detects suspicious traffic in real-time. This tool includes features like packet filtering and prioritization to further assist you in managing incoming traffic.

Indusface AppTrana

Indusface App Trana is a DDoS and bot mitigation software that provides a service bundle with a Web Application Firewall, vulnerability scanners, and patching service. It references the OWASP top 10 threats list and the SANS 25 Vulnerability list to find threats. It is also remarkably capable of handling volumetric attacks.

SolarWinds Security Event Manager

It is a DDoS protection tool that includes event log monitoring capabilities. The tool has a list of various automated features which helps the tool automatically block out available malicious IPs from dealing with your network. The list is frequently updated, ensuring your protection even from the most current threats.

Link11

Link11 is a cloud-based DDoS security tool that can identify and prevent DDoS attacks in layers 3–7. It also has a cutting-edge, AI-based attack detection method.

Cloudflare

It is a DDoS prevention tool with a network bandwidth of 30Tbps, making it more powerful than even the most powerful DDoS attacks. The tool primarily relies on its huge IP reputation database, which allows it to block malicious IPs from over 20 million locations.

Sucuri Website Firewall

It is a cheap, scalable tool that provides geo-blocking features to help you block out DDoS traffic. This tool also looks at your HTTP and HTTPS traffic to stop malicious agents from getting to your site.

StackPath Web Application Firewall

StackPath is a DDoS prevention tool and a WAP that provides layer 3, 4, and 7 protection. Behavioral algorithms are used in layer seven defense to detect and prevent volumetric threats. Its mitigation tools can block HTTP, UDP, SYN flood, and other attack channels.

Akamai Prolexic Routed

It is a security tool with zero-second mitigation, which can assist in addressing vulnerabilities as soon as they are detected. Akamai Prolexic Routed is an advanced protection tool with various features like hybrid cloud protection and is specialized for enterprises.

Techniques for DoS/DDoS Attacks

There are many techniques related to DoS and DDoS attacks. Some of them are:

UDP Flood Attack

A UDP flood attack involves an attacker dispatching forged UDP packets at an extremely high rate to a target server's random ports, utilizing a broad range of source IP addresses. This flooding of UDP packets compels the server to continuously verify the existence of applications at those ports that do not actually exist. As a result, genuine applications become unreachable, and any attempts to access them yield an error response in the form of an ICMP "Destination Unreachable" packet. This type of attack depletes network resources and bandwidth, ultimately leading to network downtime.

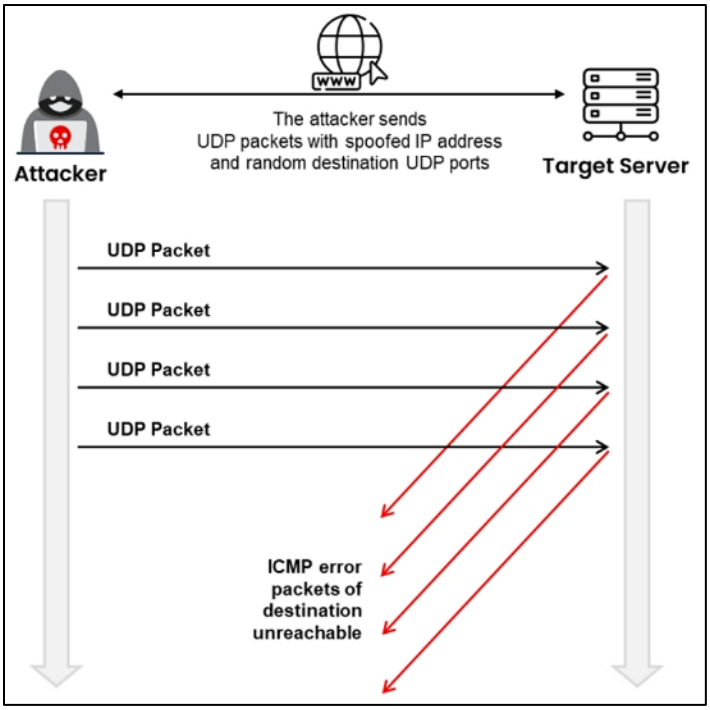

Figure 10-13: UDP Flood Attack

ICMP Flood Attack

Network administrators primarily utilize ICMP for IP operations, troubleshooting, and conveying error messages related to undeliverable packets. In an ICMP flood attack, malicious actors inundate a target system with a substantial number of ICMP echo request packets, either directly or via reflection networks. These requests prompt the target system to respond, resulting in excessive traffic that overwhelms the bandwidth of the victim's network connection, ultimately leading to a failure in responding to legitimate TCP/IP requests.

To mitigate the risk of ICMP flood attacks, it is essential to establish a threshold that activates the ICMP flood attack protection mechanism when surpassed. When the ICMP threshold is exceeded (with a default value set at 1000 packets per second), the router will deny additional ICMP echo requests from all addresses within the same security zone for the remainder of the current second and the following second.

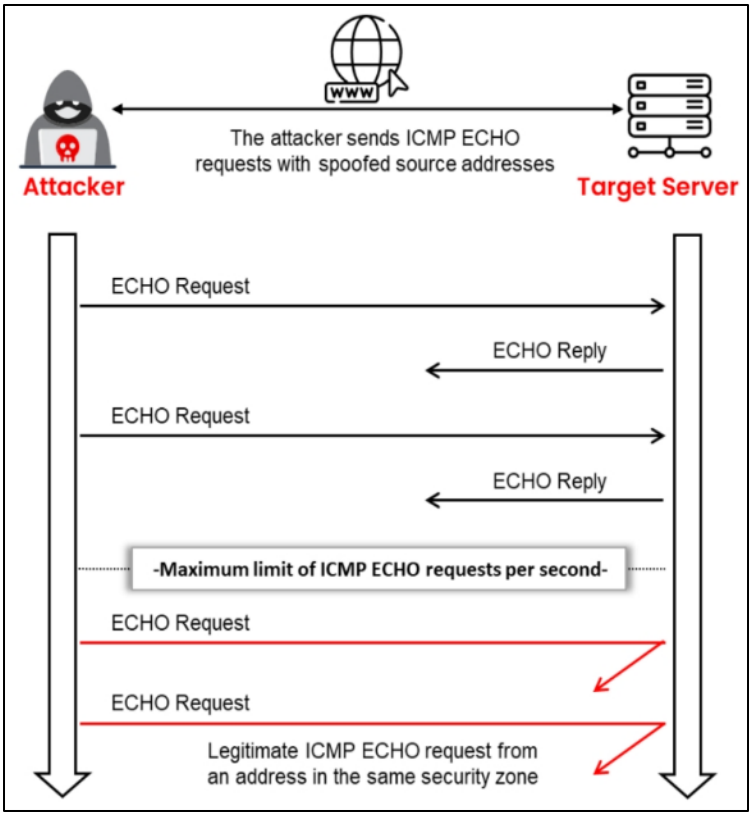

Figure 10-14: ICMP Flood Attack

Ping of Death Attack

A Ping of Death (PoD) attack involves an assailant attempting to crash, destabilize, or freeze a target system or service by dispatching malformed or excessively large packets through a basic ping command. For instance, if an attacker transmits a packet measuring 65,538 bytes to a target web server, this size surpasses the maximum limit established by RFC 791 IP, which is 65,535 bytes. The reassembly process executed by the receiving system may lead to a system crash. In these types of attacks, the identity of the attacker can be easily disguised, and the attacker typically requires minimal knowledge about the target machine, primarily its IP address.

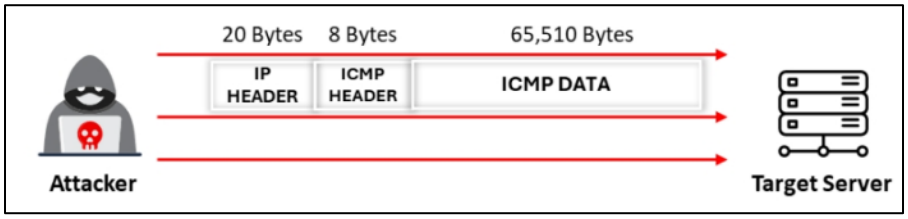

Figure 10-15: Ping of Death Attack

Smurf Attack

In a Smurf attack, the attacker falsifies the source IP address to that of the victim and sends numerous ICMP ECHO request packets to an IP broadcast network. This action prompts all hosts within the broadcast network to reply to the received ICMP ECHO requests. Since the attacker has

spoofed the IP address, these responses are directed to the victim's machine, resulting in a substantial influx of traffic that can ultimately cause the victim's machine to crash.

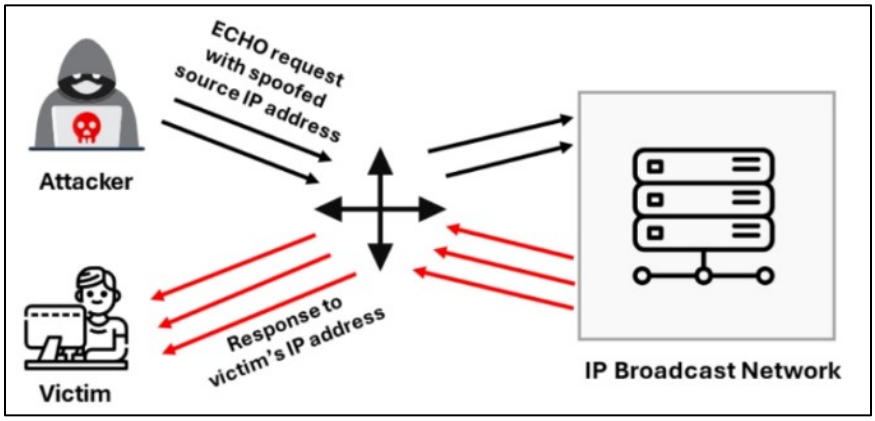

Figure 10-16: Smurf Attack

Pulse Wave DDoS Attack

Pulse wave DDoS attacks represent the latest type of DDoS assaults utilized by malicious actors to interfere with the normal functioning of their targets. Unlike traditional DDoS attack patterns characterized by a continuous influx of traffic, pulse wave DDoS attacks exhibit a periodic pattern, delivering substantial bursts of traffic that can overwhelm the target's bandwidth. Attackers transmit a highly repetitive sequence of packets in pulses every ten minutes, with the duration of the attack session ranging from approximately one hour to several days. A single pulse can exceed 300 Gbps, sufficient to saturate a network connection. Recovery from such attacks poses significant challenges and may, in some cases, be unfeasible.

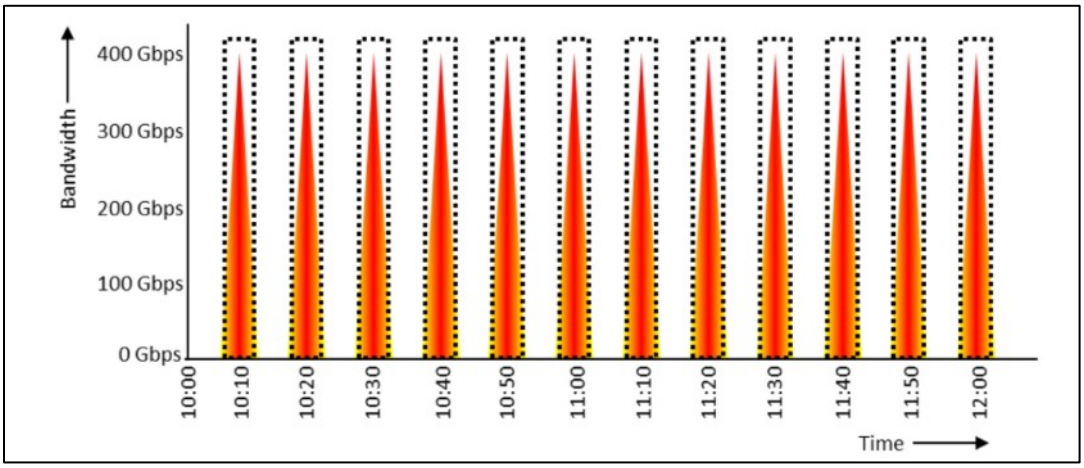

Figure 10-17: Pulse Wave DDoS Attack

Zero-Day DDoS Attack

Zero-day DDoS attacks occur when vulnerabilities associated with DDoS are unpatched and lack effective defensive measures. During these attacks, the threat actor exploits the vulnerability while the victim remains unaware, actively blocking the victim's resources and exfiltrating sensitive data. Such attacks can inflict considerable harm on the victim's network infrastructure and assets.

Presently, there is no comprehensive strategy available to safeguard networks against this type of attack.

NTP Amplification Attack

The Network Time Protocol (NTP) is essential for synchronizing time across various networked systems, including host machines, processes, and devices. It plays a critical role in maintaining accurate timekeeping, which is vital for numerous network operations, protocols, and logging activities. In an NTP amplification attack, an attacker employs a botnet to dispatch large UDP packets using a spoofed IP address that resembles the victim's actual IP address to the NTP server. This type of attack typically exploits an NTP server with the monlist command enabled. Each UDP packet sent prompts a request to the NTP server via the monlist command, resulting in the generation of substantial response packets. The server then promptly replies to the spoofed IP address, leading to the victim's IP address being overwhelmed with these large responses. This inundation causes the surrounding network infrastructure to be flooded with excessive traffic, ultimately resulting in a denial-of-service condition characterized by network congestion, service interruptions, and the depletion of network resources such as bandwidth, memory, and power.

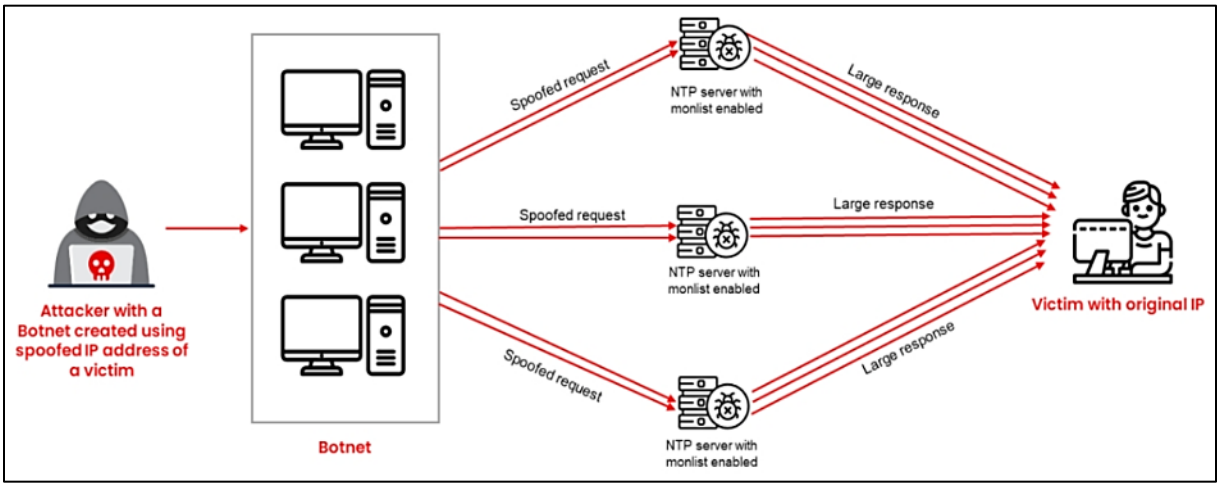

Figure 10-18: Illustration of NTP Server Amplification Attack

Steps to obtain the monlist from an NTP server:

- Execute the following command to access the monlist: **nmap -sU -pU:123 -Pn -n --script=ntp-monlist <target>**
- Upon running the command, Nmap will display a list of both public and private clients that have interacted with the NTP server.

Countermeasures Against NTP Amplification Attacks:

- Fortify and secure NTP server configurations to mitigate the risk of monlist exploitation
- Regulate flow control within the NTP server
- Regularly monitor the network for any unusual activities
- Adopt a zero-trust network approach
- Employ firewalls to filter requests directed at the NTP server

SYN Flood Attack

A SYN flood attack involves an assailant dispatching a substantial volume of SYN requests to a targeted server, utilizing counterfeit source IP addresses. This tactic results in the establishment of incomplete TCP connections, thereby depleting network resources. Typically, when a client seeks to initiate a TCP connection with a server, a sequence of messages is exchanged:

- The client transmits a TCP SYN request packet to the server
- The server replies with a SYN/ACK (acknowledgment) in response to the request
- The client then sends an ACK back to the server, finalizing the session setup

This interaction is known as the "**three-way handshake.**"

In a SYN flood attack, the attacker takes advantage of this three-way handshake process. Initially, the attacker sends a fraudulent TCP SYN request to the target server. Upon receiving this request, the server responds with a SYN/ACK, but the attacker does not follow up with an ACK response. Consequently, the server remains in a state of anticipation, waiting to finalize the connection.

SYN flooding exploits the vulnerabilities inherent in the way most hosts execute the TCP three-way handshake. The attack is characterized by the attacker sending an overwhelming number of SYN packets to the host system at a rate that exceeds the system's capacity to manage. Under normal circumstances, a connection is established through the TCP three-way handshake, during which the host monitors partially open connections while awaiting response ACK packets in a listening queue. As illustrated, when Host B receives a SYN request from Host A, it must maintain a record of the partially opened connection in a "listen queue" for a minimum duration of 75 seconds.

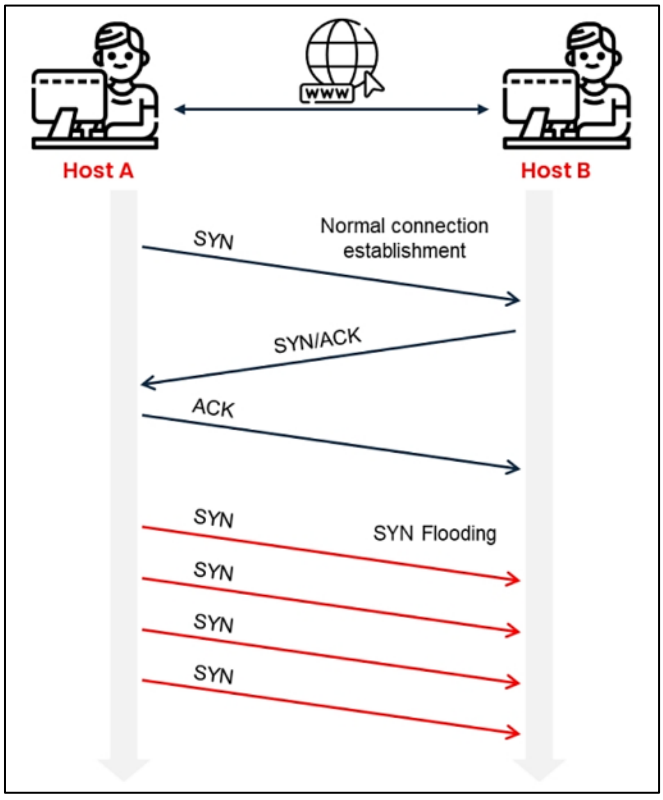

Figure 10-19: SYN Flood Attack

A malicious host can compromise another host by managing numerous partial connections through the simultaneous transmission of multiple SYN requests to the target host. Once the connection queue reaches its capacity, the system is unable to establish new connections until it discards some entries from the queue due to handshake timeouts. This capacity to maintain each incomplete connection for 75 seconds can be systematically exploited in a Denial-of-Service (DoS) attack. The attack employs forged IP addresses, complicating the tracing of its origin. An attacker can populate a connection table even without the need to spoof the source IP address.

In addition to SYN flood attacks, adversaries may also utilize SYN-ACK and ACK/PUSH ACK flood attacks to disrupt the operations of target machines. While these attacks share similar functionalities, they exhibit minor variations.

SYN-ACK Flood Attack

This attack resembles the SYN flood attack; however, it specifically targets the second phase of the three-way handshake. The attacker inundates the target machine with a significant volume of SYN-ACK packets, thereby depleting its resources.

ACK and PUSH ACK Flood Attack

In the context of an active TCP session, the ACK and PUSH ACK flags facilitate the transfer of information between the server and client machines until the session concludes. In an ACK and PUSH ACK flood attack, attackers overwhelm the target machine with a substantial number of spoofed ACK and PUSH ACK packets, rendering it inoperative.

Countermeasures for SYN Flood Attacks

Proper packet filtering is a practical approach to mitigate SYN flood attacks. Additionally, an administrator may adjust the TCP/IP stack to minimize the effects of SYN attacks while still accommodating legitimate client traffic.

Some SYN attacks aim not to disrupt servers but rather to exhaust the total bandwidth of the Internet connection. To combat this type of attack, tools such as SYN cookies and SynAttackProtect can be employed. To further protect against an attacker seeking to deplete bandwidth, an administrator might consider implementing supplementary safety measures. For instance, reducing the timeout duration for pending connections in the "SYN RECEIVED" state can be beneficial. Typically, if a client fails to send a response ACK, the server will resend the initial ACK packet. This vulnerability can be mitigated by shortening the retransmission time for the first packet, limiting the number of retransmissions, or completely disabling packet retransmissions.

Fragmentation Attack

This type of attack undermines a victim's ability to reconstruct fragmented packets by flooding them with TCP or UDP fragments, leading to reduced performance. In fragmentation attacks, the attacker sends a substantial number of fragmented packets (exceeding 1500 bytes) to a targeted web server at a relatively low packet rate. Given that the protocol permits fragmentation, these packets typically evade scrutiny as they traverse network devices such as routers, firewalls, and Intrusion Detection/Prevention Systems (IDS/IPS). The process of reassembling and inspecting these large,

fragmented packets demands considerable resources. Additionally, the attacker randomizes the content within the packet fragments, further increasing the resource consumption required for reassembly and inspection, ultimately resulting in system failure.

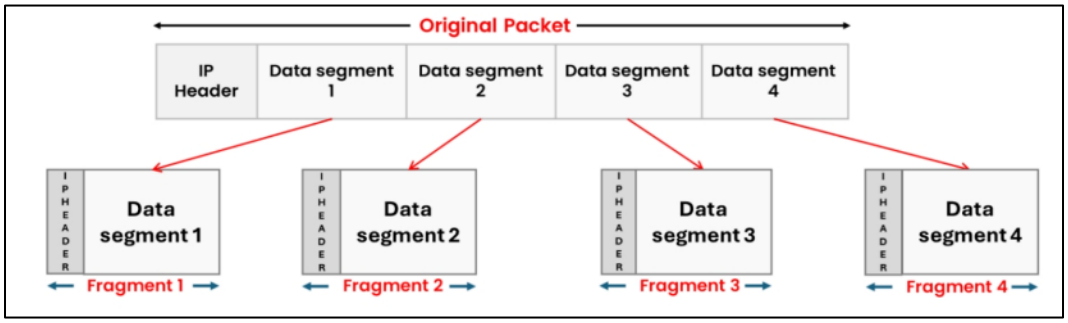

Figure 10-20: Fragmentation Attack

Spoofed Session Flood Attack

This attack involves the creation of counterfeit or spoofed TCP sessions by sending numerous SYN, ACK, and RST or FIN packets. Attackers utilize this method to circumvent firewalls and execute Distributed Denial-of-Service (DDoS) attacks on targeted networks, thereby depleting their network resources. Below are examples of spoofed session flood attacks:

- **Multiple SYN-ACK Spoofed Session Flood Attack:** In this variant, attackers establish a fraudulent session by transmitting multiple SYN and ACK packets, accompanied by one or more RST or FIN packets.
- **Multiple ACK Spoofed Session Flood Attack:** In this variant, attackers initiate a fake session by omitting SYN packets entirely and relying solely on multiple ACK packets, along with one or more RST or FIN packets. Since SYN packets are not utilized, and given that firewalls predominantly employ SYN packet filters to identify irregular traffic, the detection rate for these types of DDoS attacks by firewalls is significantly low.

HTTP GET/POST Attack

HTTP attacks are classified as layer-7 attacks. HTTP clients, including web browsers, establish connections to a web server via HTTP to transmit requests, which can be categorized as either HTTP GET or HTTP POST. Malicious actors take advantage of these requests to execute Denial-of-Service (DoS) attacks. In an HTTP GET attack, the perpetrator employs a time-delayed HTTP header to maintain an HTTP connection, thereby depleting the resources of the web server. The attacker refrains from sending the complete request to the target server, resulting in the server holding the HTTP connection open and waiting, which renders it inaccessible to legitimate users. During such attacks, all network parameters may appear normal, yet the service remains unavailable. In an HTTP POST attack, the attacker transmits HTTP requests that include full headers but lack a complete message body to the targeted web server or application. Due to the incomplete message body, the server continues to wait for the remainder, causing the web server or application to be unavailable to legitimate users. An HTTP GET/POST attack represents a complex layer-7 attack that does not rely on malformed packets, spoofing, or reflection techniques. This type of attack necessitates less bandwidth compared to other forms of attacks to incapacitate

the targeted site or web server. The objective of this attack is to force the server to allocate maximum resources to address the attack, thereby denying legitimate users access to the server's resources.

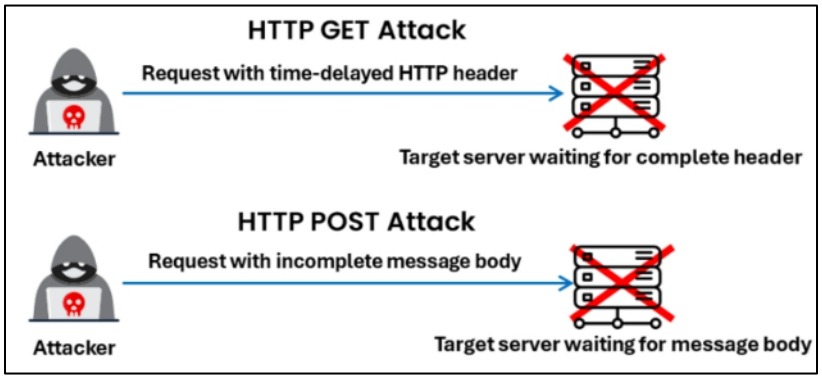

Figure 10-21: HTTP GET/POST Attack

In addition to the previously mentioned HTTP GET/POST attack, attackers may use various HTTP flood attacks to exhaust the bandwidth of the target network:

Single-Session HTTP Flood Attack

This attack method involves an attacker taking advantage of vulnerabilities in HTTP 1.1 to bombard a target with numerous requests within a single HTTP session.

Single-Request HTTP Flood Attack

In this scenario, the attacker generates multiple HTTP requests from a single session by embedding these requests within a single HTTP packet. This approach enables the attacker to remain anonymous and undetected while executing DDoS attacks.

Recursive HTTP GET Flood Attack

Maintaining a low profile is crucial for attackers. By masquerading as a legitimate user and engaging in seemingly valid actions, an attacker can trick firewalls into perceiving the source as authentic. The recursive GET method compiles a list of pages or images, simulating navigation through them while

stealthily launching flooding attacks on the target. When combined with an HTTP flood attack, the recursive GET can inflict significant damage on the target.

Random Recursive GET Flood Attack

This type of recursive GET flood attack is specifically tailored for forums, blogs, and other sequentially organized websites. Similar to the recursive GET flood attack, this method involves the recursive GET appearing to browse through pages. Targeting forums, groups, and blogs, the attacker employs random numbers within a valid page range to impersonate a legitimate user, sending a new GET request with each iteration. In both recursive GET and random recursive GET flood attacks, the target is overwhelmed with a multitude of GET requests, leading to resource exhaustion.

Slowloris Attack

Slowloris is a tool designed for executing DDoS attacks at layer 7, specifically aimed at disrupting web infrastructure. Unlike other DDoS tools, it uses legitimate HTTP traffic to incapacitate a target server. In a Slowloris attack, the attacker transmits incomplete HTTP requests to the intended web server or application. As the server receives these partial requests, it establishes multiple connections and remains in a state of anticipation for the requests to finalize. However, since the requests are never completed, the server's maximum limit for concurrent connections becomes saturated, resulting in the denial of further connection attempts.

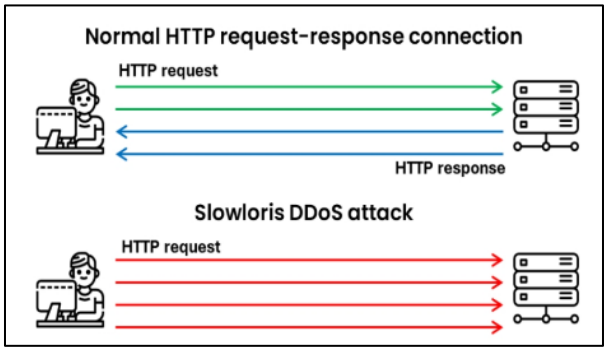

Figure 10-22: Slowloris Attack

UDP Application Layer Flood Attack

While UDP flood attacks are primarily recognized for their volumetric characteristics, certain application layer protocols that use UDP can be exploited by attackers to execute flood attacks against targeted networks. Below are examples of UDP-based application layer protocols that can be utilized for such flooding attacks:

- Character Generator Protocol (CHARGEN)
- Simple Network Management Protocol Version 2 (SNMPv2)
- Quote of the Day (QOTD)
- Remote Procedure Call (RPC)
- SSDP
- Connection-less Lightweight Directory Access Protocol (CLDAP)
- Trivial File Transfer Protocol (TFTP)
- Network Basic Input/Output System (NetBIOS)
- NTP
- Quake Network Protocol
- Steam Protocol
- Voice over Internet Protocol (VoIP)

Multi-Vector Attack

In multi-vector Distributed Denial-of-Service (DDoS) attacks, the attacker employs a mix of volumetric, protocol, and application layer attacks to incapacitate the intended system or service. The attacker rapidly shifts from one type of DDoS attack, such as SYN packets, to another, targeting layer 7. These attacks may be executed sequentially through a single vector or simultaneously across

multiple vectors, thereby disorienting the organization's IT department and forcing them to exhaust their resources while diverting their attention.

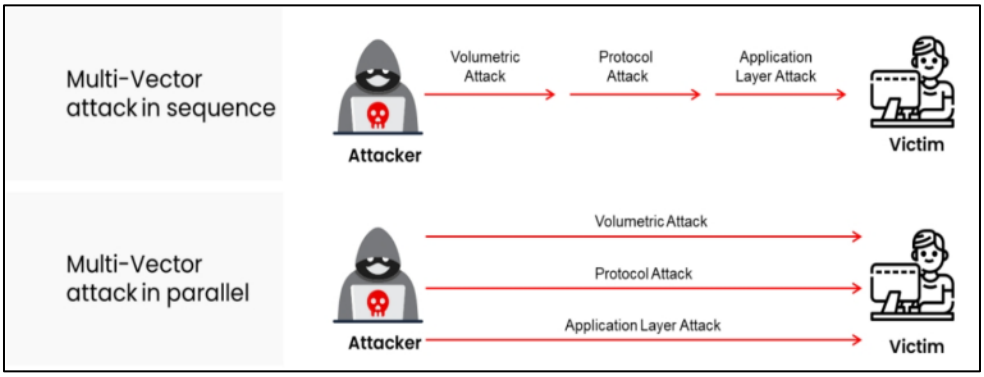

Figure 10-23: Multi-Vector Attack

Peer-to-Peer Attack

A peer-to-peer attack represents a specific type of Distributed Denial-of-Service (DDoS) attack wherein the perpetrator takes advantage of vulnerabilities present in peer-to-peer servers to initiate the attack. Attackers target weaknesses in networks utilizing the Direct Connect (DC++) protocol, which facilitates file sharing among instant messaging clients. This method of attack does not rely on botnets. In contrast to botnet-driven assaults, a peer-to-peer attack allows attackers to bypass direct communication with the compromised clients. Instead, the attacker directs users of substantial peer-to-peer file-sharing networks to sever their connections to the network and redirect them to the victim's website. As a result, thousands of computers may simultaneously attempt to access the targeted site, leading to a significant degradation in its performance. Peer-to-peer attacks can be readily identified through their distinct signatures. By employing this strategy, attackers can execute extensive DoS attacks aimed at disrupting websites.

To mitigate the risk of peer-to-peer DDoS attacks, it is advisable to designate specific ports for peer-to-peer communications. For instance, restricting communication to port 80 can effectively reduce the possibility of such attacks impacting websites.

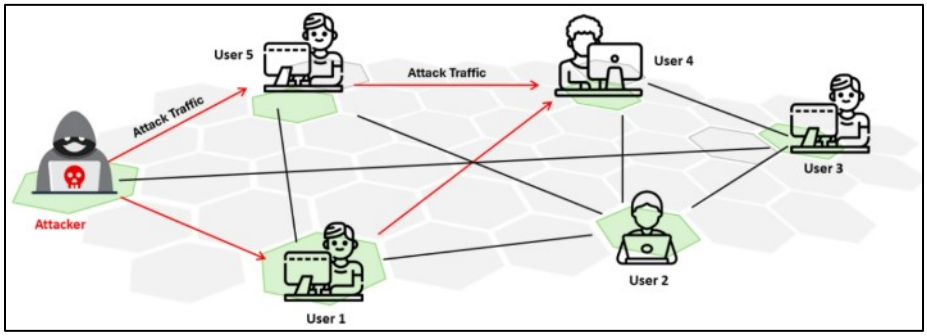

Figure 10-24: Peer to Peer Attack

Permanent Denial-of-Service Attack

Permanent Denial-of-Service (PDoS) attacks, commonly referred to as phlashing, specifically target hardware components, resulting in irreversible damage. Unlike traditional DoS attacks, which

primarily disrupt services, PDoS attacks compromise the physical hardware, necessitating its replacement or reinstallation. These attacks exploit vulnerabilities within a device, enabling unauthorized remote access to management interfaces of the affected hardware, including printers, routers, and various networking devices.

PDoS attacks are characterized by their rapid execution and destructive potential, surpassing the impact of standard DoS attacks. They require fewer resources compared to Distributed Denial-of-Service (DDoS) attacks, which deploy a network of compromised systems against a target. The methodology employed in PDoS attacks involves a technique known as "bricking." In this approach, attackers disseminate fraudulent communications—such as emails, IRC messages, tweets, or videos—purporting to be legitimate hardware updates. These updates are intentionally altered to include vulnerabilities or faulty firmware. When the victim interacts with the deceptive link or pop-up window associated with the fraudulent update, they inadvertently install it, granting the attacker full control over the victim's system.

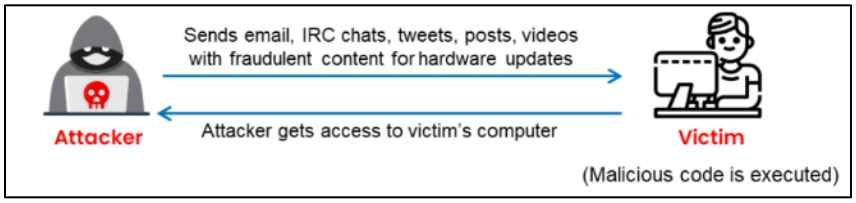

Figure 10-25: Permanent DoS Attack

TCP SACK Panic Attack

The TCP Selective Acknowledgment (SACK) panic attack represents a remote attack strategy wherein attackers aim to crash a targeted Linux system by dispatching SACK packets that contain improperly configured Maximum Segment Sizes (MSS). This method exploits an integer overflow vulnerability present in the Linux Socket Buffer (SKB), potentially resulting in a kernel panic. Typically, Linux systems implement the TCP SACK protocol, which allows the sender to be informed of the packets that the receiver has successfully acknowledged. Consequently, the sender is able to retransmit only those packets that have not been acknowledged. In this context, Linux utilizes a linked-list data structure known as the socket buffer to retain data until it is acknowledged or received. The socket buffer can hold a maximum of 17 segments, after which the acknowledged packets are promptly removed from the linked structure. If the socket buffer attempts to accommodate more than 17 segments, it may trigger a kernel panic. The TCP SACK panic attack exploits this specific vulnerability within the socket buffer. To execute this attack, adversaries send meticulously crafted SACK packets in succession to the target server, configuring the MSS to the minimal value of 48 bytes. This minimal MSS value results in an increased number of TCP segments requiring retransmission. Such selective retransmission can cause the target server's socket buffer to surpass its 17-segment limit, leading to an integer overflow and subsequent kernel panic that leads to a DoS. Given that the vulnerability lies within the kernel stack, this attack can also be directed against containers and virtual machines.

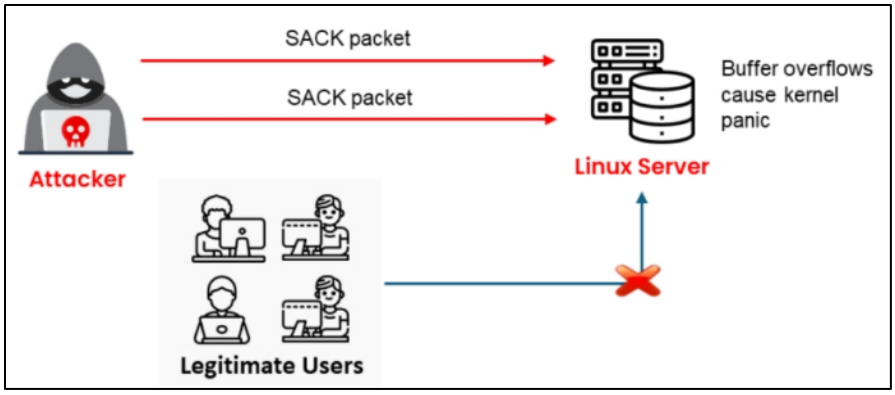

Figure 10-26: TCP SACK Panic Attack

Countermeasures

- Apply vulnerability patches
- Establish a firewall rule to prevent the acceptance of packets that have the lowest MSS

Distributed Reflection Denial-of-Service (DRDoS) Attack

A Distributed Reflection Denial-of-Service (DRDoS) attack, often referred to as a "spoofed" attack, uses numerous intermediary and secondary systems to facilitate a DDoS attack on a designated target machine or application. This type of attack takes advantage of the vulnerabilities exploited in the TCP three-way handshake process. The architecture of a DRDoS attack comprises an attacking machine, intermediary victims (often termed zombies), secondary victims (known as reflectors), and the primary target machine.

The attack is initiated when the attacker instructs the intermediary victims to dispatch a series of packets (TCP SYN) that falsely present the primary target's IP address as the source IP to other unaffected machines (the secondary victims or reflectors). This action prompts the reflectors to attempt to establish a connection with the primary target, resulting in a substantial influx of traffic (SYN/ACK) directed at the primary target under the false assumption that the target initiated the request.

Upon receiving the SYN/ACK packets from the reflectors, the primary target discards them, as it did not send the corresponding SYN packet. Meanwhile, the reflectors, believing that the initial packet was lost, continue to resend SYN/ACK packets to the primary target in an effort to establish a connection until a timeout occurs. This process leads to the target machine being inundated with excessive traffic from the reflectors, as the cumulative bandwidth of these machines significantly overwhelms the target.

The DRDoS attack is particularly sophisticated, as it is challenging, if not impossible, to trace the actual attacker. Instead of the true perpetrator, the secondary victims (reflectors) appear to be the ones directly assaulting the primary target. This method proves to be more effective than conventional DDoS attacks due to the substantial attack bandwidth generated by multiple intermediary and secondary victims.

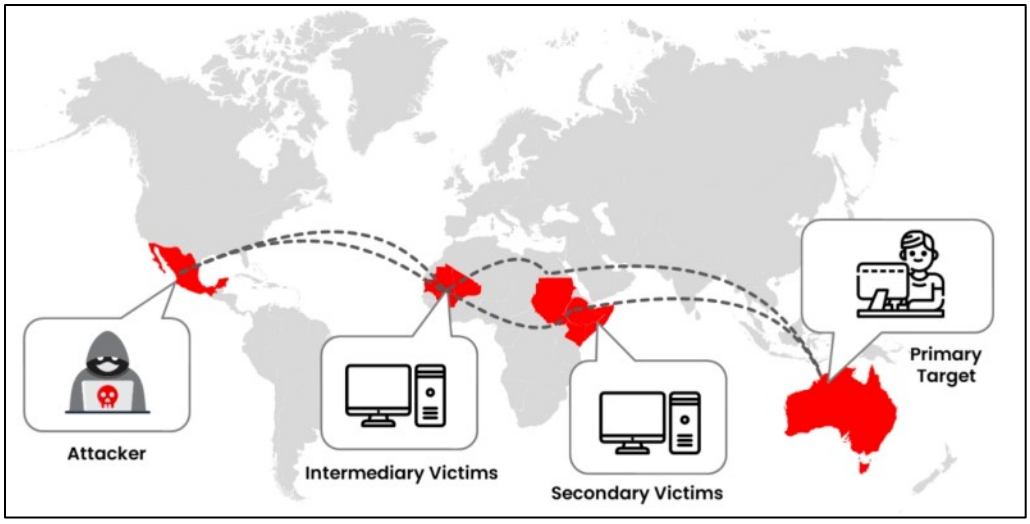

Figure 10-27: Distributed Reflection DoS (DRDoS) Attack

Countermeasures

- Disable the Character Generator Protocol (CHARGEN) service to mitigate this attack vector
- Ensure that the latest updates and patches for servers are installed

DDoS Extortion/Ransom DDoS (RDDoS) Attack

The DDoS extortion attack, commonly known as Ransom DDoS (RDDoS), involves attackers threatening targeted organizations with a DDoS attack unless a specified ransom is paid. The attacker may either issue a ransom note or conduct a preliminary DDoS attack using a botnet on particular resources of the organization to instill a sense of urgency regarding the threat. Following this, the victim receives an email containing a ransom or extortion note detailing payment options, deadlines, and warnings that the full-scale attack could be executed at any time. The ransom note may also feature brief messages or a series of threats concerning vulnerabilities, exposed assets, or sensitive data, along with instructions for making the ransom payment via digital currency. Typically, attackers exaggerate their capabilities, asserting that they possess advanced DDoS tools capable of inflicting significant harm to the organization's operations.

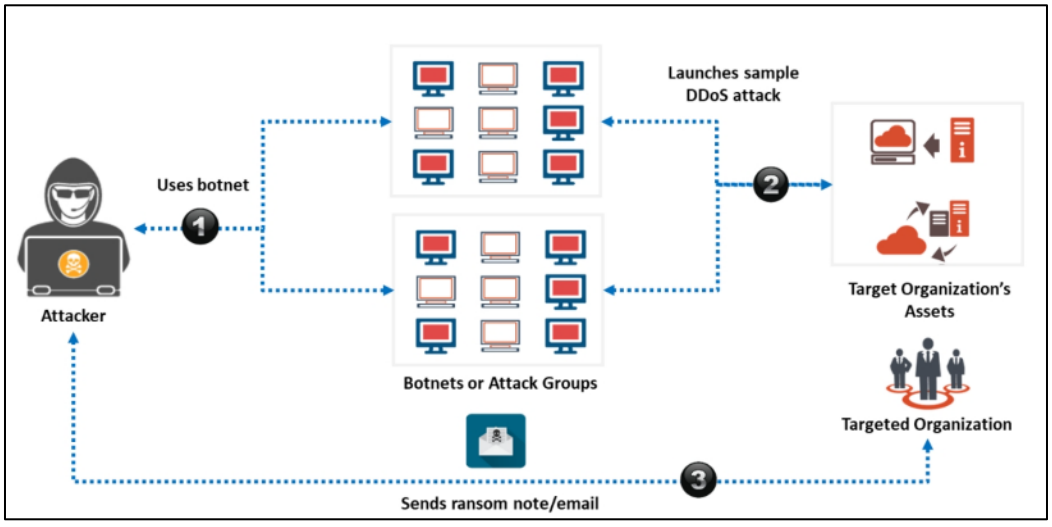

Figure 10-28: DDoS Extortion Attack

Countermeasures

- Deploy robust DDoS protection solutions
- Promptly notify law enforcement and security personnel upon receipt of a ransom demand
- Regularly assess assets to determine risk tolerance
- Establish mitigation strategies, including BGP/DNS redirection and continuous protection services

DoS/DDoS Attack Toolkits Available in the Wild

ISB

The ISB (I'm So Bored) software utility enables attackers to execute DDoS attacks against a designated network. This tool facilitates various types of flood attacks, including HTTP, UDP, TCP, and ICMP, targeting the network. Additionally, it offers convenient one-click access to frequently utilized network commands such as WHOIS, netstat, traceroute, and ping, assisting attackers in identifying their targets.

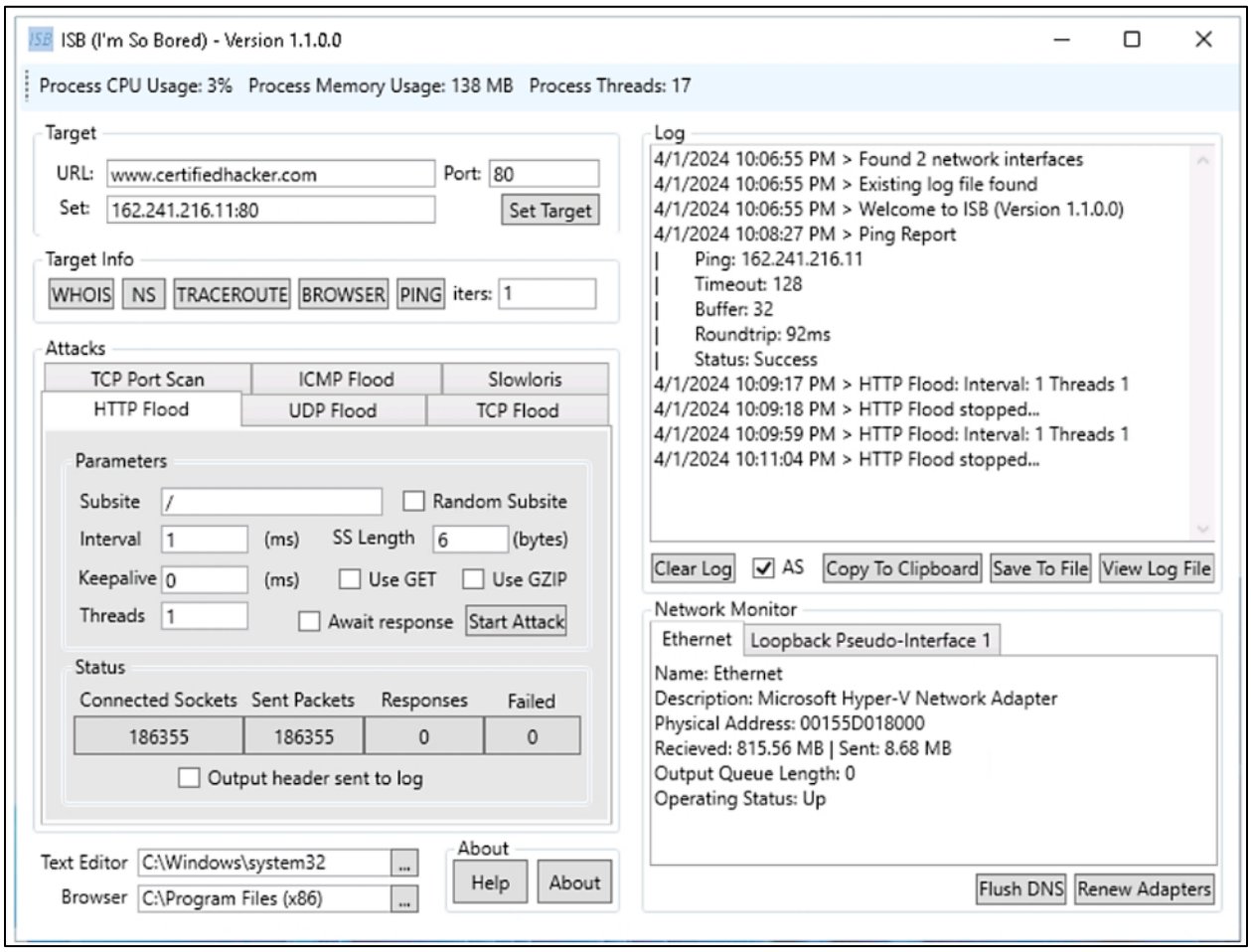

Figure 10-29: Screenshot of ISB DoS Attack Tool

UltraDDOS-v2

UltraDDOS-v2 is a tool designed for executing Distributed Denial-of-Service (DDoS) attacks against targeted websites or servers. It features an intuitive Graphical User Interface (GUI) that allows users to input the target's IP address, specify the port number, and determine the desired packet transmission volume.

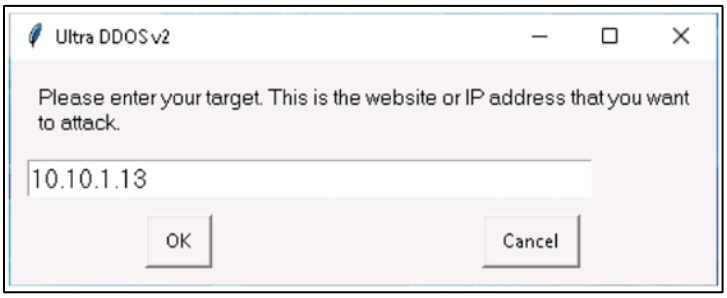

Figure 10-30: Screenshot of Target IP Address Specified on UltraDDOS-v2

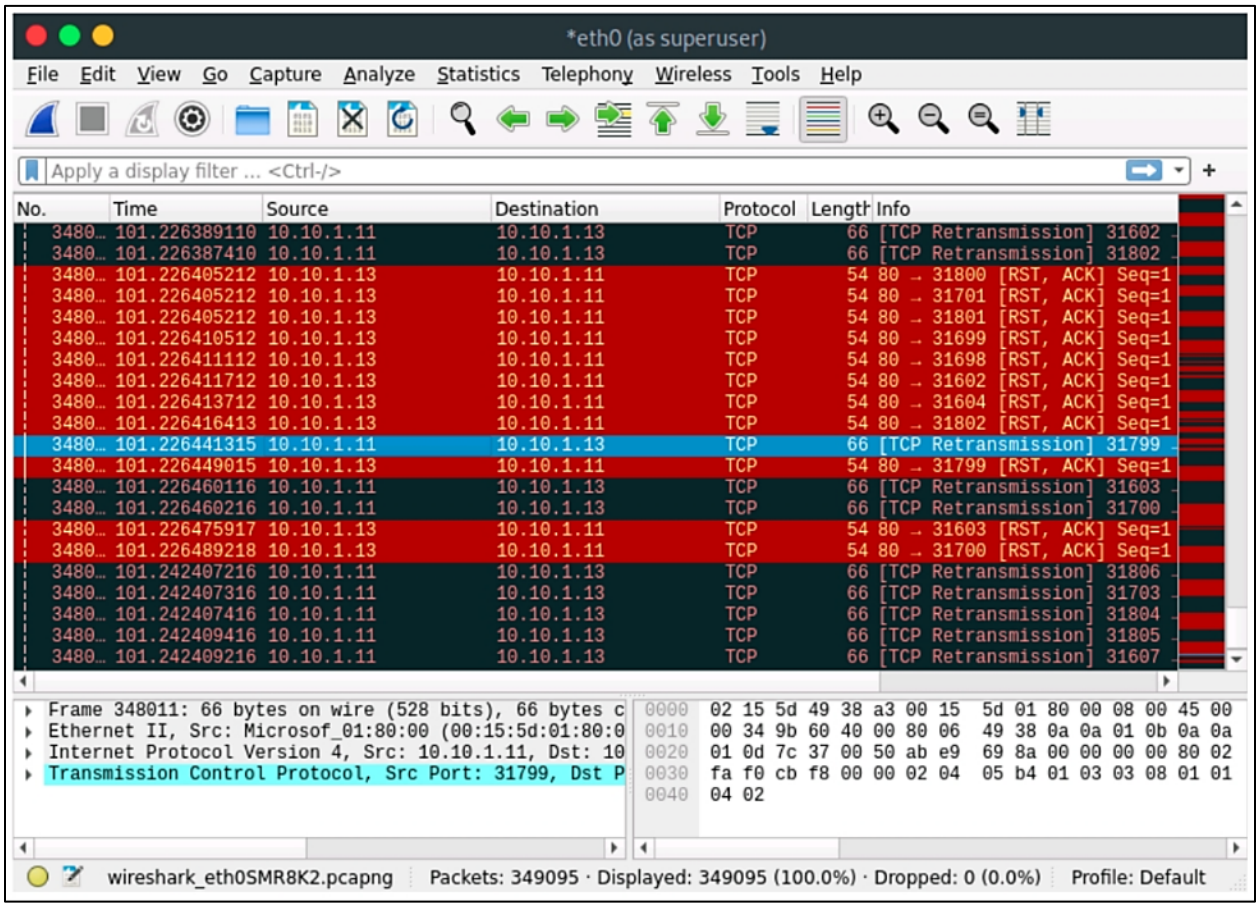

Figure 10-31: Flood Recorded on the Target Machine

Additionally, there are several other tools available for conducting DoS/DDoS attacks, including:

- High Orbit Ion Cannon (HOIC)
- Low Orbit Ion Cannon (LOIC)

- HULK
- Slowloris
- UFONet
- Packet Flooder Tool

DoS/DDoS Attack Countermeasures

DoS and DDoS attacks represent significant security challenges on the Internet, necessitating the development of effective mitigation strategies. This section explores detection techniques, a range of preventive measures, responses to DoS/DDoS incidents, and the hardware and software tools available for protecting networks against such attacks.

Detection Techniques

Early detection methods are crucial in preventing DoS/DDoS attacks. Identifying a DoS/DDoS attack presents significant challenges. A traffic detection system for DoS/DDoS attacks must differentiate between legitimate and fraudulent data packets, a task that is not always feasible. Consequently, the techniques utilized for detection are inherently imperfect. There remains a possibility of misidentifying traffic from legitimate network users as that generated by a DoS/DDoS attack. These detection methods rely on recognizing and distinguishing between an illegitimate surge in traffic and legitimate packet transmission. One of the primary challenges in filtering out fraudulent traffic from legitimate sources is the sheer volume of data. It is impractical to examine each data packet individually to safeguard against DoS/DDoS attacks. Current detection techniques characterize an attack as a significant and observable deviation in network traffic patterns and statistics. These methods employ statistical analysis to identify and classify malicious traffic versus legitimate traffic. The following are three categories of detection techniques:

Activity Profiling

Activity profiling is conducted based on the average packet rate within network flows, which consist of consecutive packets sharing similar header information. This header information encompasses the IP addresses of both the sender and recipient, as well as the ports and transport protocols utilized. An attack is signaled by:

- An increase in activity levels among network flow clusters
- A rise in the total number of distinct clusters (indicative of a DDoS attack)

For a higher average packet rate or increased activity level within a flow, the interval between successive matching packets diminishes. Variability in the average packet rate or activity level may suggest potentially malicious behavior. The entropy calculation method serves to quantify the randomness in activity levels. An escalation in the entropy of network activity levels may signify that the network is experiencing an attack.

A significant challenge in the activity profiling approach is the substantial volume of traffic. This issue can be addressed by clustering packet flows that exhibit similar characteristics. Given that Denial-of-Service (DoS) attacks produce a vast number of nearly identical data packets, an uptick in the average packet rate or an increase in packet diversity could be indicative of such an attack.

Sequential Change-Point Detection

The sequential change-point detection method involves filtering network traffic based on IP addresses, targeted port numbers, and utilized communication protocols. The resulting traffic flow data is represented in a graph that plots the traffic flow rate against time. Change-point detection algorithms are employed to identify alterations in network traffic statistics and flow rates that may result from attacks. A significant shift in traffic flow rate could suggest the occurrence of a DoS attack. This technique utilizes the Cumulative Sum (CUSUM) algorithm to detect and pinpoint DoS attacks by calculating discrepancies between the actual and expected local averages in the traffic time series. Additionally, the sequential change-point detection method can recognize typical scanning behaviors associated with network worms.

Wavelet-Based Signal Analysis

The wavelet analysis technique examines network traffic through its spectral components. It decomposes incoming signals into various frequency ranges and analyzes each frequency component independently. By assessing the energy within each spectral window, anomalies can be detected. These techniques evaluate the frequency components present at specific times and provide insights into those components. The detection of an unfamiliar frequency may indicate suspicious activity within the network.

DoS/DDoS Mitigation Approaches

- **Attack Absorption:** This approach involves utilizing additional capacity to absorb the impact of an attack, necessitating prior planning and the allocation of extra resources. A notable drawback of this method is the financial burden associated with maintaining these resources, which persists even in the absence of attacks.
- **Service Degradation:** When maintaining full service functionality during an attack proves unfeasible, prioritizing the operation of essential services is advisable. This entails identifying critical services and subsequently modifying the network, systems, and application designs to minimize the operation of non-essential services. This strategy can aid in ensuring that vital services remain operational.
- **Service Suspension:** This approach entails the complete shutdown of all services until the attack has ceased. While it may not represent the most favorable option, it can be a pragmatic response in certain situations.

DDoS Attack Countermeasures

Numerous strategies have been suggested to alleviate the impact of DDoS attacks. Nonetheless, there is no singular, comprehensive solution capable of safeguarding against all recognized types of DDoS attacks. Furthermore, attackers are constantly developing innovative techniques to execute DDoS attacks that can circumvent existing security measures. Below are examples of countermeasures against DDoS attacks:

- Protect secondary victims
- Identify and neutralize handlers
- Avert potential attacks
- Redirect attacks

- Alleviate attacks
- Conduct post-attack forensics

Protecting Secondary Victims

Individual Users

The most effective approach to prevent DDoS attacks is for systems identified as secondary victims to ensure they do not participate in the attack. This demands heightened security awareness and the implementation of preventive measures. Secondary victims should consistently monitor their security protocols to protect against DDoS agent software. It is crucial to prevent the installation of any DDoS agent programs and to ensure that DDoS agent traffic does not infiltrate the network. Regular installation and updates of antivirus and anti-Trojan software, along with timely software patches to address known vulnerabilities, are essential.

Additionally, enhancing awareness of security concerns and preventive strategies among all Internet users is vital. It is important to disable unnecessary services, remove unused applications, and thoroughly scan all files received from external sources. Although these tasks may seem overwhelming for the average web user, the fundamental hardware and software of computing systems are equipped with integrated defenses against the insertion of malicious code. Therefore, it is imperative that these built-in protective mechanisms are properly configured and routinely updated to mitigate the risk of DDoS attacks. By implementing these countermeasures, attackers will be deprived of a DDoS attack network from which to launch their attacks.

Network Service Providers

Service providers and network administrators may implement dynamic pricing models for network usage, allowing them to charge potential secondary victims for Internet access. This approach aims to motivate users to take proactive measures to prevent themselves from being involved in DDoS attacks.

Detect and Neutralize Handlers

A crucial strategy for mitigating DDoS attacks involves the detection and neutralization of handlers. This can be accomplished through network traffic analysis, the neutralization of botnet handlers, and the identification of spoofed source addresses. In the context of agent-handler DDoS attack tools, the handler serves as an intermediary for the attacker to launch attacks. By analyzing communication protocols and traffic patterns between handlers and clients or between handlers and agents, it is possible to identify the network nodes compromised by the handlers. Locating and disabling these handlers can serve as an effective means of disrupting the DDoS attack network. Given that the number of DDoS handlers is significantly lower than that of agents, neutralizing a limited number of handlers can potentially render multiple agents, thereby mitigating DDoS attacks. Additionally, there is a substantial likelihood that the spoofed source addresses of DDoS attack packets do not correspond to valid source addresses within the specific sub-network. Identifying these spoofed addresses, combined with a comprehensive understanding of communication protocols and traffic among handlers, clients, and agents, can effectively prevent DDoS attacks.

Mitigating Potential Threats

Egress Filtering

Egress filtering involves examining the headers of IP packets that are leaving a network. Packets that meet established criteria are permitted to leave the originating sub-network, while those that do not meet the required specifications are blocked from reaching their intended destination. This process is crucial in preventing unauthorized or harmful traffic from exiting the internal network. Distributed Denial-of-Service (DDoS) attacks often utilize spoofed IP addresses. Implementing protocols that mandate any legitimate packet departing from a company's network to possess a source address that aligns with the internal network can significantly reduce the risk of such attacks. A well-configured firewall for the sub-network can effectively filter out numerous DDoS packets that have spoofed source addresses. In cases where a web server is susceptible to a zero-day exploit known only within the underground hacking community, the server may remain vulnerable despite the application of all available security patches. However, by enabling egress filtering, users can protect the integrity of their systems by preventing the server from establishing a connection back to the attacker. This measure also diminishes the effectiveness of various payloads commonly used in exploits. By restricting outbound traffic to only what is necessary, the potential for attackers to connect to additional systems and access tools that facilitate further infiltration into the network is significantly limited.

Ingress Filtering

Ingress filtering is a method of packet filtering employed by numerous Internet Service Providers (ISPs) to mitigate the risk of source address spoofing in Internet traffic. By implementing ingress filtering, ISPs can indirectly address various forms of network abuse, as it allows for the tracing of Internet traffic back to its genuine source. This technique also offers protection against flooding attacks that may arise from legitimate IP address prefixes, thereby facilitating the identification of the true originator.

TCP Intercept

TCP intercept is a feature found in routers designed to safeguard TCP servers from SYN-flooding attacks, a specific type of Denial-of-Service (DoS) attack. During a SYN-flooding attack, an attacker inundates the server with a large number of connection requests that utilize unreachable return addresses. Since these addresses cannot be reached, the connections remain unresolved, leading to an overwhelming number of open connections that can incapacitate the server, preventing it from servicing legitimate requests. To counter this, TCP intercept mode allows a router to capture the SYN packets directed at a server and compare them against an extended access list. If a match is found, the intercept software establishes a connection with the client on behalf of the destination server while simultaneously creating a connection with the server on behalf of the client. Once these two half-connections are formed, the intercept software seamlessly merges them. This process effectively prevents fraudulent connection attempts from reaching the server, as the intercept software acts as an intermediary throughout the connection.

Rate Limiting

Rate limiting is a method employed to manage the flow of outbound or inbound traffic through a network interface controller. This approach effectively mitigates the excessive volume of incoming traffic that can lead to a Distributed Denial-of-Service (DDoS) attack. It is particularly crucial to implement this method in hardware appliances, where it is configured to restrict the rate of requests at layers 4 and 5 of the Open Systems Interconnection (OSI) model.

Deflecting Attacks

Systems designed with minimal security, commonly referred to as honeypots, serve as bait for potential attackers. Recent studies indicate that a honeypot can replicate all facets of a network, encompassing web servers, mail servers, and client systems. These honeypots are deliberately established with reduced security measures to attract DDoS attackers, allowing for the collection of valuable information regarding the attackers, their techniques, and the tools they utilize by documenting system activities. DDoS attackers drawn to a honeypot may deploy handlers or agent code within it, thereby preventing the compromise of more sensitive systems. Honeypots not only safeguard the actual system from intruders but also monitor and record the attackers' activities. As a result, the owner of the honeypot can maintain a log of the handler and/or agent interactions. This information can be utilized to bolster defenses against potential future DDoS attacks. A defense-in-depth strategy utilizing Internet Protocol Security (IPsec) can be implemented at various network junctures to redirect suspicious Denial-of-Service (DoS) traffic to multiple honeypots. There are two primary categories of honeypots:

- Low-interaction honeypots
- High-interaction honeypots

An example of a high-interaction honeypots is a honeynet. Honeynets constitute a vital component of security infrastructure; they replicate the entire configuration of a computer network specifically designed to "capture" attacks. The primary objective is to establish a network where all actions are monitored and recorded. This network includes decoys that serve as potential victims, and it also incorporates actual computers operating genuine applications.

Blumira Honeypot Software

Blumira honeypot software represents a type of deception technology designed to help security professionals identify unauthorized access attempts and monitor the lateral movement of attackers within an organization's network, particularly in the event of a breach. This software contributes to the enhancement of the organization's security maturity and facilitates early detection of attacks, all while requiring minimal maintenance and resources. Upon identifying a honeypot security incident, Blumira promptly blocks the originating IP address at the switch or firewall level.

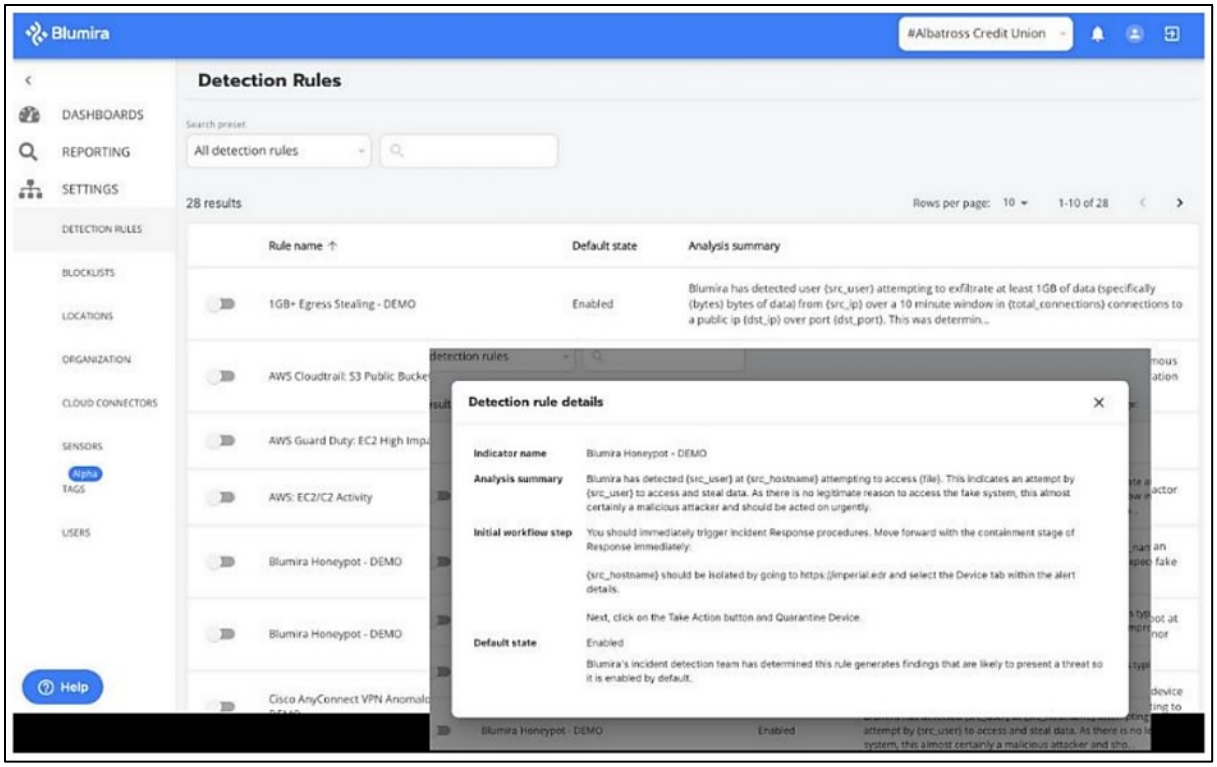

Figure 10-32: Blumira Honeypot Software

Additional examples of DoS/DDoS countermeasure tools that utilize honeypot technology include:

- KFSensor
- Valhala Honeypot
- Cowrie
- HoneyHTTPD
- StingBox

Mitigating Attacks

Load Balancing

Bandwidth providers can enhance bandwidth on essential connections during a DDoS attack, thereby safeguarding their servers from potential shutdowns. Implementing a replicated server model offers an additional layer of protection. These replicated servers facilitate improved load management by distributing workloads across multiple servers, which not only enhances overall network performance but also diminishes the impact of a DDoS attack.

Throttling

Throttling involves configuring routers to manage server access by regulating incoming traffic levels to ensure they remain within safe limits for the server. The "min-max fair server-centric router" employs throughput controls to help users avert server shutdowns. This technique is effective in mitigating server damage by managing DoS traffic. Throttling enables routers to handle substantial incoming traffic, ensuring that the server can cope with it. Furthermore, it distinguishes legitimate user traffic from fraudulent DDoS attack traffic and can be adapted to limit DDoS traffic

while permitting legitimate user traffic for optimal outcomes. A significant drawback of this approach is the potential for false alarms, which may occasionally allow harmful traffic to bypass filters while blocking some legitimate requests.

Drop Requests

An alternative strategy involves discarding packets when the server's load increases. Typically, the router or server executes this task. However, prior to processing a request, the system may require the requester to solve a complex puzzle that demands considerable memory or computational resources. As a result, users operating compromised systems may experience a decline in performance, which could deter them from participating in the transmission of DDoS attack traffic.

Post-Attack Forensics

Traffic Pattern Analysis

The traffic pattern tool records post-attack data during a DDoS attack, which users can examine to find features specific to the attacking traffic. The efficiency and protective capacity of load balancing and throttling countermeasures can be updated with the use of these data. Furthermore, network administrators can create new filtering strategies to stop DDoS attack traffic from entering or exiting their networks by using the patterns of DDoS attack traffic. Network administrators can also make sure that an attacker cannot use their servers as a DDoS platform to compromise other websites by analyzing DDoS traffic patterns.

Packet Traceback

Packet traceback involves the process of tracing the origin of attack traffic, similar to reverse engineering. In this approach, the targeted entity retraces the path of the packets to identify their source. Once the genuine source is determined, the victim can implement measures to prevent future attacks from that origin by establishing appropriate countermeasures. Moreover, packet traceback can provide insights into the various tools and techniques employed by the attacker, which can be valuable for developing and applying diverse filtering strategies to block such attacks.

Event Log Analysis

DDoS event logs play a crucial role in forensic investigations and legal enforcement, particularly in cases where the attacker inflicts significant financial harm. Service providers can utilize honeypots and other network security tools, including firewalls, packet sniffers, and server logs, to document all events that transpired during the planning and execution of the attack. This documentation enables network administrators to identify the specific type of DDoS attack or the combination of attacks that were executed. By analyzing logs from routers, firewalls, and intrusion detection systems, administrators can trace the source of the DoS traffic. Additionally, they may collaborate with intermediary ISPs and law enforcement agencies to trace the attacker's IP address.

Techniques for Protecting Against Botnets

There are four primary methods for protecting against botnets:

RFC 3704 Filtering

RFC 3704 serves as a fundamental Access Control List (ACL) filter that mitigates the effects of DDoS attacks by blocking traffic originating from spoofed addresses. This filter mandates that packets must originate from valid, allocated address spaces that align with the network's topology and allocation. A "bogon list" comprises all unused or reserved IP addresses that should not be present on the Internet. If a packet is traced back to any IP address on the bogon list, it is deemed to originate from a spoofed source, and the filter is designed to discard it. System administrators should verify whether their Internet Service Provider (ISP) implements RFC 3704 filtering prior to the traffic entering their systems. Given that the bogon list is subject to frequent updates, if the ISP does not provide RFC 3704 filtering, the system administrator must either manage their own bogon ACL rules or consider switching to a different ISP.

Cisco IPS Source IP Reputation Filtering

Reputation services play a crucial role in assessing whether an IP address or service poses a threat. Cisco Global Correlation, a recent enhancement in Cisco IPS 7.0, leverages extensive security intelligence. The Cisco SensorBase Network contains data regarding all known threats on the Internet, including botnets, malware outbreaks, dark nets, and botnet harvesters. The Cisco IPS utilizes this network to filter Denial-of-Service (DoS) traffic before it can compromise critical assets. To enhance the detection and prevention of malicious activities at an earlier stage, it integrates global threat data into its operational framework.

Black Hole Filtering

Black-hole filtering is a widely utilized strategy to mitigate the impact of botnets and, consequently, to avert Denial-of-Service (DoS) attacks. The term "black holes" refers to network nodes that discard incoming traffic without notifying the source that the data has failed to reach its intended destination. A technique known as Remotely Triggered Black Hole (RTBH) filtering allows for the elimination of undesirable traffic before it infiltrates a secured network. This process is initiated remotely and necessitates collaboration with the Internet Service Provider (ISP). It employs Border Gateway Protocol (BGP) host routes to redirect traffic intended for the victim's servers to a "nullo" next hop.

DDoS Prevention Solutions from ISPs or DDoS Service Providers

This approach is effective in countering IP spoofing at the ISP level. In this scenario, the ISP cleanses the traffic before it is permitted to enter a user's Internet connection. As this service operates in the cloud, it ensures that DDoS attacks do not overwhelm the Internet links. Additionally, various third-party providers offer cloud-based DDoS prevention services. Features such as IP Source Guard (available in CISCO) or similar functionalities in other routers can be activated to filter traffic based on the DHCP snooping binding database or IP source bindings, thereby preventing bots from transmitting spoofed packets.

Additional DoS/DDoS Mitigation Strategies

The implementation of defensive strategies in appropriate locations adhering to established protocols, significantly enhances the security of an organization's network. Below is a compilation of strategies aimed at mitigating DoS/DDoS attacks:

- Use robust encryption standards such as WPA2/WPA3 and AES 256 for broadband networks to safeguard against eavesdropping
- Regularly update software and protocols and conduct comprehensive scans of systems to identify any irregular activities
- Upgrade the kernel to the most recent version and deactivate any unused or vulnerable services
- Block all incoming packets from service ports to prevent traffic from reflection servers
- Activate TCP SYN cookie protection
- Prevent the transmission of spoofed packets at the Internet Service Provider (ISP) level
- Utilize cognitive radios at the physical layer to counteract jamming and scrambling attacks
- Configure firewalls to restrict access to external Internet Control Message Protocol (ICMP) traffic
- Ensure secure remote administration and connectivity testing
- Conduct rigorous input validation
- Avoid the use of unnecessary functions such as gets and strcpy
- Use cutting-edge network-level surveillance technologies to oversee the network perimeter
- Use that semi-accessible connection is equipped with robust timeout mechanisms
- Adopt a distributed server architecture and colocation services as a contingency model to mitigate server overload during DDoS attacks
- Verify that the servers are devoid of bottlenecks and points of failure
- Engage third-party protection services to enhance security against significant DDoS attacks
- Utilize multi-cloud deployment strategies for critical applications to guarantee adequate backup during DDoS incidents on cloud platforms
- Conduct comprehensive simulations of DoS/DDoS attacks to prevent unexpected surges and maintain an effective countermeasure strategy
- Exchange information with industry counterparts and utilize threat intelligence feeds to remain informed about DDoS attack patterns
- Implement AI/ML and anomaly detection systems to recognize automatically and flag irregularities in typical traffic behavior
- Restrict network broadcasting and deactivate services such as echo and chargen

DoS/DDoS Protection at the ISP Level

A highly effective strategy for mitigating DoS attacks involves intercepting them at the gateway, a responsibility typically managed by the contracted Internet Service Provider (ISP). ISPs provide a "clean pipes" service-level agreement, which guarantees a bandwidth allocation for legitimate traffic, as opposed to the total bandwidth encompassing all traffic. In many instances, ISPs may opt to block all incoming requests during a DDoS attack, which, unfortunately, includes legitimate traffic attempting to access the service. In cases where an ISP does not offer clean-pipes services, organizations can utilize subscription services from various cloud service providers. These services

act as intermediaries, filtering incoming traffic and allowing only trusted connections to proceed to the network. Companies such as Imperva and VeriSign are notable vendors that provide cloud-based protection against DoS attacks.

Additionally, ISPs offer in-the-cloud DDoS protection for Internet connections to prevent saturation during an attack. This protective measure involves redirecting attack traffic to the ISP, allowing administrators to request the blocking of the original affected IP address and subsequently migrate their site to a different IP after completing DNS propagation.

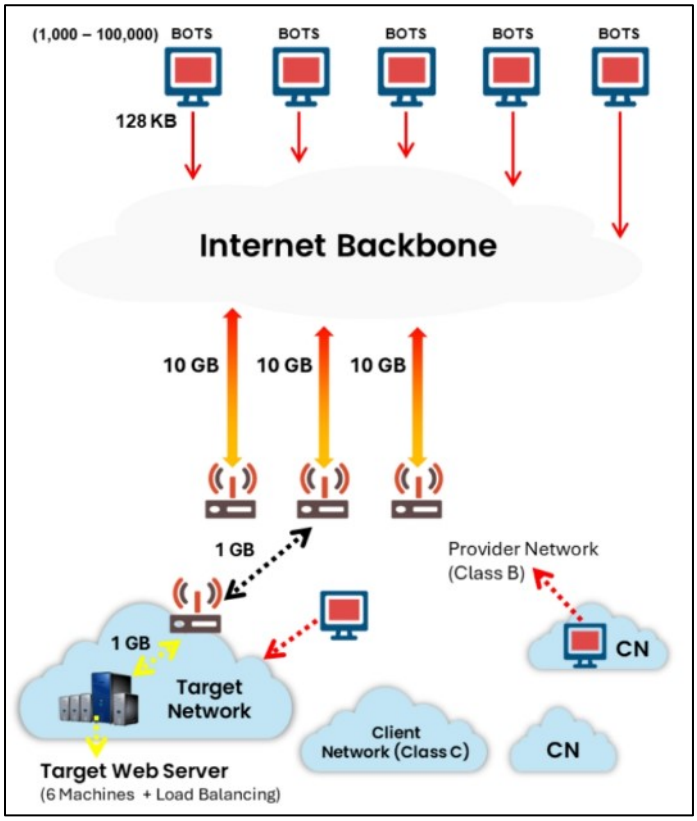

Figure 10-33: DoS/DDoS Protection At the ISP Level

Enabling TCP Intercept on Cisco IOS Software

TCP intercept can be activated by entering the commands listed in the table below while in global configuration mode.

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

Table 10-01: Steps to Enable TCP Intercept on Cisco IOS

An access list serves three primary functions:

1. Interception of all incoming requests
2. Interception of requests originating from designated networks only

3. Interception of requests directed towards specific servers only

An access list generally designates the source as any origin while specifying particular networks or servers as the destination. The identification of source addresses is not critical for intercepting packets; thus, they remain unfiltered. Instead, the focus is on identifying the destination server or network that requires protection. TCP intercept can function in two modes: active intercept mode and passive watch mode, with the default setting being the intercept mode.

In active intercept mode, the Cisco IOS software proactively intercepts all incoming connection requests (SYN) and responds with an SYN-ACK on behalf of the server, subsequently awaiting an Acknowledgment (ACK) from the client. Upon receiving the ACK from the client, the server transmits the original SYN, allowing the software to establish a three-way handshake with the server. Once this handshake is completed, the two half-connections are connected.

In passive watch mode, the user initiates connection requests that traverse the server, but these requests must wait until the connection is fully established. Should the connection requests fail to establish within 30 seconds, the software issues a reset request to the server to terminate its current state.

The following table outlines the command necessary to configure the TCP intercept mode in global configuration mode.

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

Table 10-02: TCP Intercept Mode In The Global Configuration Mode

Advanced DDoS Protection Appliances

The following appliances exemplify advanced protection against DDoS attacks:

FortiDDoS 200F, 1500E, 1500E-DC, 1500F, 2000E, 2000E-DC, and VM04/08/16

FortiDDoS employs a highly parallel machine-learning architecture that provides superior and low-latency mitigation of DDoS attacks, avoiding the performance drawbacks typically associated with CPU-based systems. It thoroughly inspects both inbound and outbound packets across Layers 3, 4, and 7, down to the smallest sizes, ensuring rapid and precise detection and mitigation.

Figure 10-34: FortiDDoS 1500F

Quantum DDoS Protector

Check Point's Quantum DDoS Protector offers multi-layered protection to effectively block DDoS attacks. Its key features include:

- Comprehensive attack blocking through tailored multi-layered protection
  - Behavioral protection that establishes baselines across multiple elements to identify and block abnormal traffic
  - Predefined and automatically generated signatures
  - Implementation of advanced challenge/response techniques
- Rapid response capabilities to counteract attacks within seconds
  - Automatic defense against both network floods and application layer attacks
  - Customized protection tailored to the specific security requirements of a network environment
  - Efficient traffic filtering prior to reaching the firewall, safeguarding networks and servers while blocking potential exploits
- Versatile deployment options suitable for any business
- Seamless integration with Check Point Security Management

Huawei AntiDDoS1000 DDoS Protection System

The Huawei AntiDDoS1000 is a sophisticated DDoS protection system that leverages Big Data analytics to effectively model over 60 different types of network traffic. It provides a rapid, second-level response to attacks and offers comprehensive protection against more than 100 distinct attack vectors. This system can be implemented within a user's network in an in-line mode, enabling real-time defense against both volumetric and application-layer attacks. In instances where the attack traffic surpasses the bandwidth or the defensive capacity of a local scrubbing device, the AntiDDoS1000 collaborates with the upstream carrier or ISP's AntiDDoS device to mitigate flood attacks and ensure uninterrupted service.

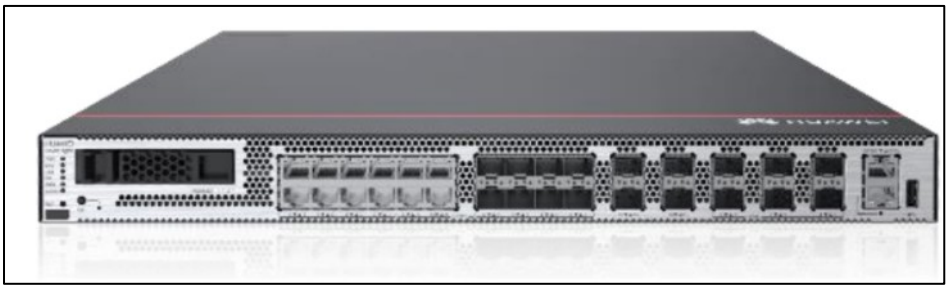

Figure 10-35: Huawei AntiDDoS1000 DDoS Protection System

A10 Thunder TPS

A10 Thunder Threat Protection System (TPS) guarantees dependable access to essential network services by identifying and mitigating external threats, including DDoS attacks and other cyber threats before they escalate into expensive service disruptions. The system offers the following features:

- Ensures service continuity
- Counteracts increasing threats
- Provides scalable defense
- Lowers security operational expenditures

Figure 10-36: A10 Thunder TPS

DDoS Protection Solutions

Anti DDoS Guardian

Anti DDoS Guardian serves as a protective measure against DDoS attacks. It protects various types of servers, including IIS servers, Apache servers, gaming servers, Camfrog servers, mail servers, FTP servers, VOIP PBX systems, SIP servers, and other comparable infrastructures. This tool conducts real-time monitoring of all incoming and outgoing packets, providing details such as local and remote addresses along with additional network flow information. Anti DDoS Guardian imposes restrictions on the number of network flows, client bandwidth, the number of concurrent TCP connections per client, and the rate of TCP connections. Furthermore, it regulates UDP bandwidth, UDP connection rates, and the rate of UDP packets.

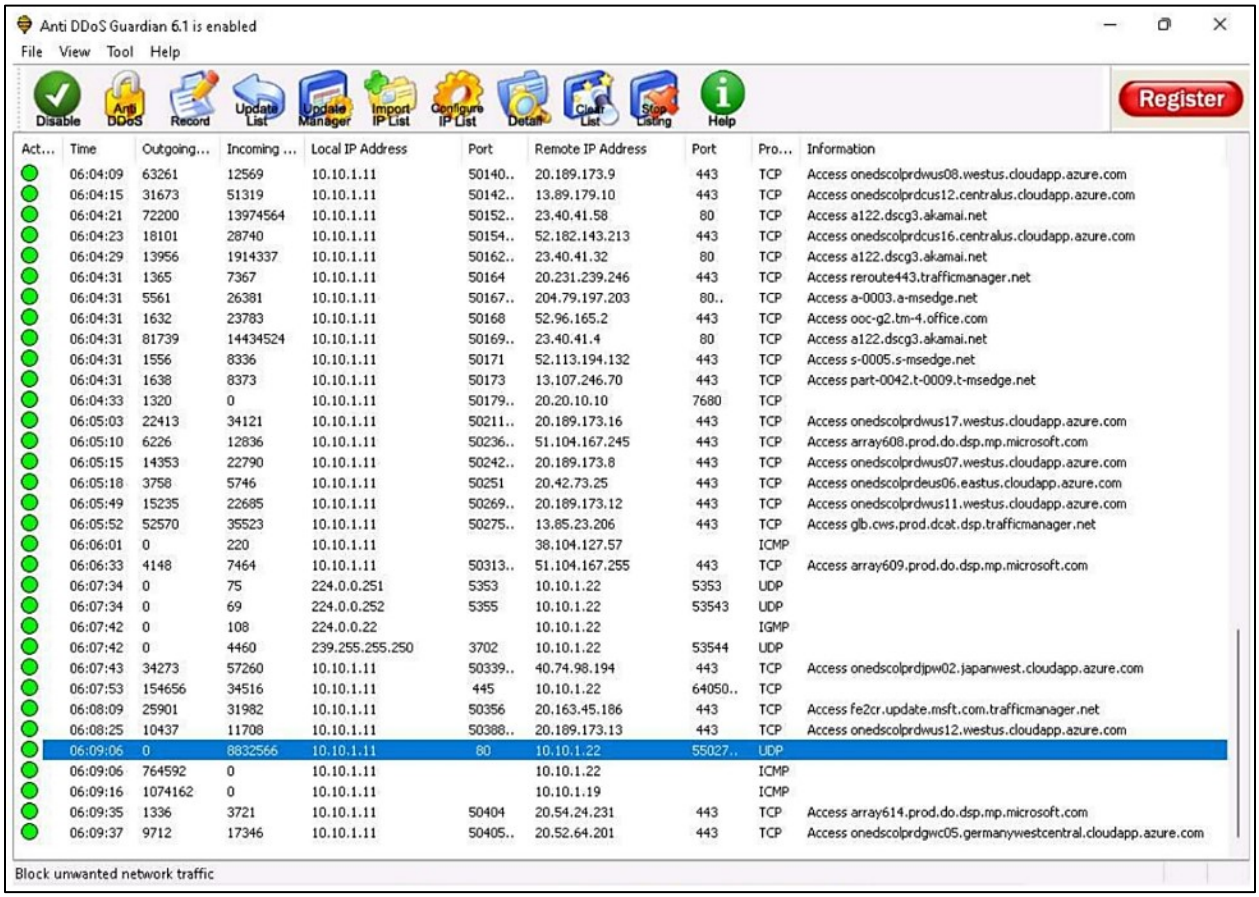

Figure 10-37: Screenshot of Anti DDoS Guardian

DDoS Protection Services

Cloudflare

Cloudflare offers a robust DDoS protection service designed to assist organizations in safeguarding their networks from distributed denial-of-service attacks. This service utilizes a 100 Tbps network capable of blocking approximately 87 billion threats each day. Rapid mitigation is achieved in as little as three seconds, and it employs sophisticated methods, including BGP-based protection and integration with Layer 7 services, to ensure thorough security while minimizing operational expenses.

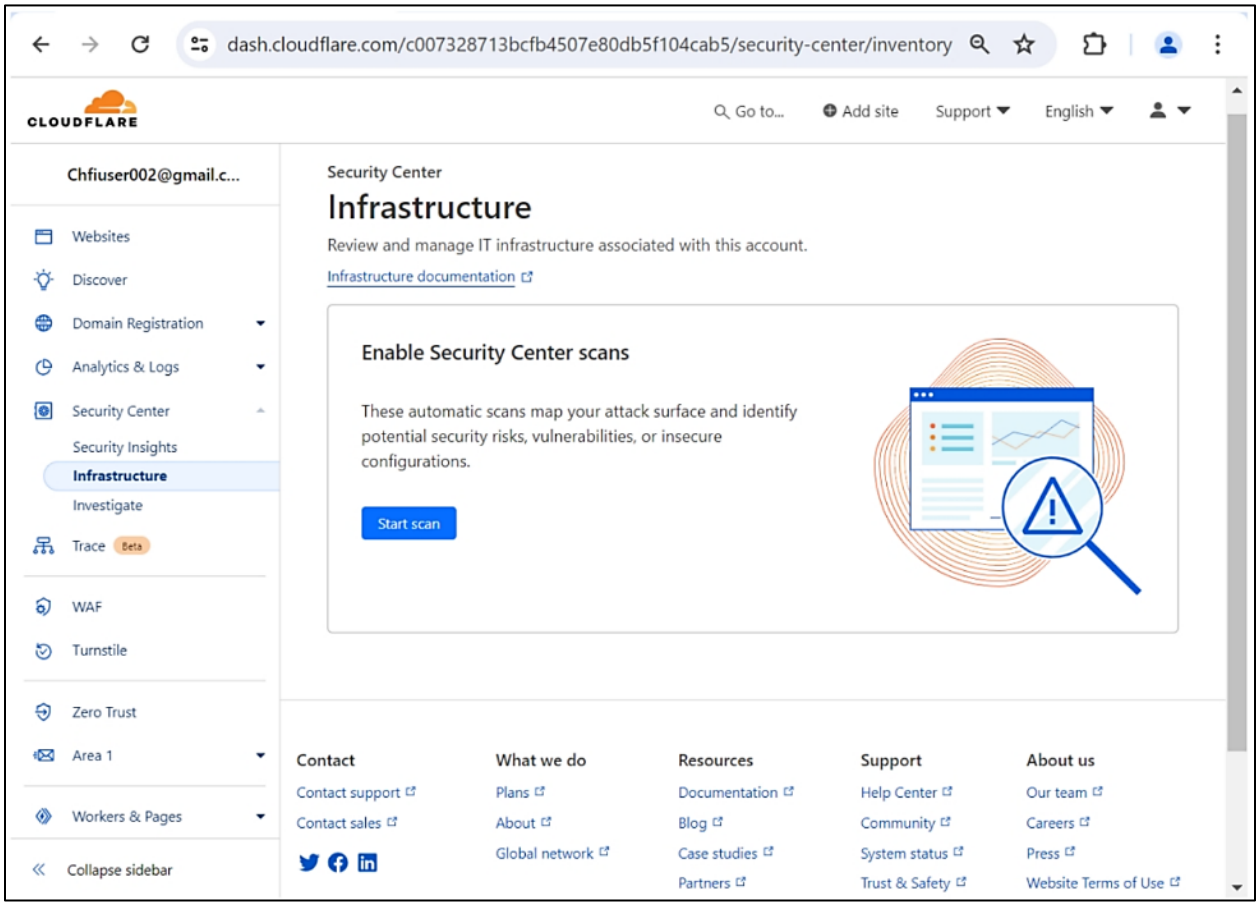

Figure 10-38: Screenshot of Cloudflare Dashboard

Akamai DDoS Protection

Akamai DDoS Protection used specialized infrastructure to protect Internet-facing applications and systems while providing rapid, secure, and consistently available DNS services. This solution effectively mitigates DDoS attacks and harmful traffic in the cloud, preventing them from impacting applications, data centers, and infrastructure, thereby removing the need for numerous firewalls.

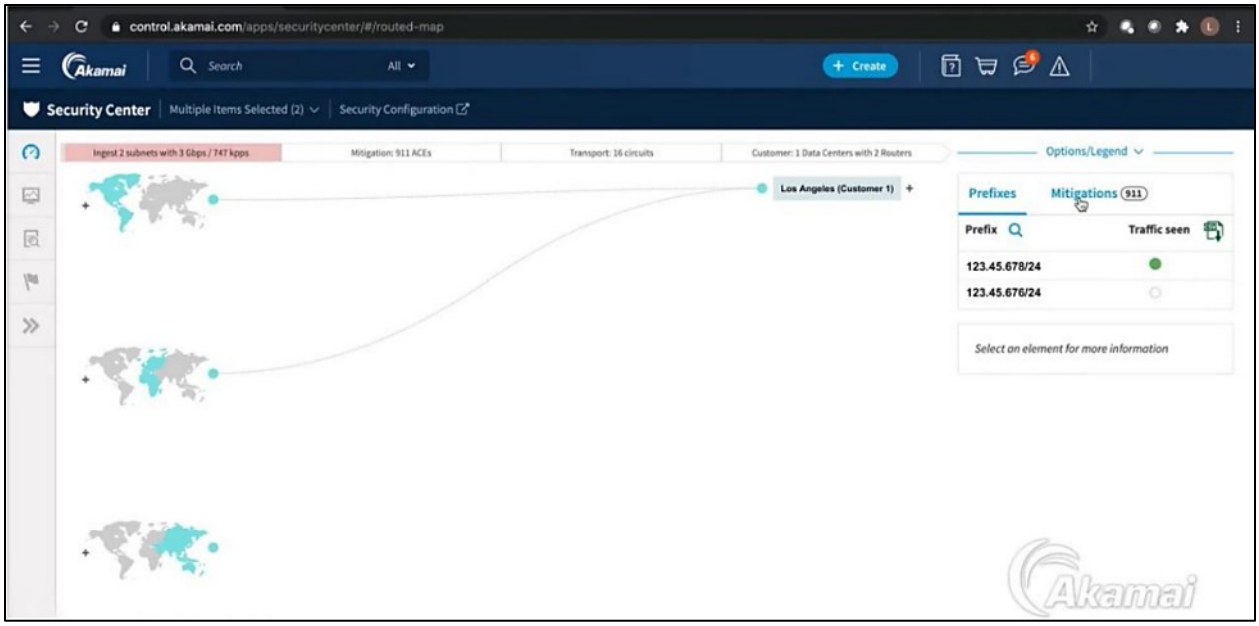

Figure 10-39: Screenshot of Akamai Console

Summary

In this chapter, we explored the concepts of Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks, along with an overview of botnets and their ecosystem. We also examined various DoS/DDoS attack tools and the different types of these attacks. Additionally, a comprehensive case study on the Google Cloud HTTP/2 'Rapid Reset' attack was presented. The chapter concluded with an in-depth discussion of countermeasures to mitigate DoS/DDoS attacks, including both hardware and software protection tools.

Mind Map

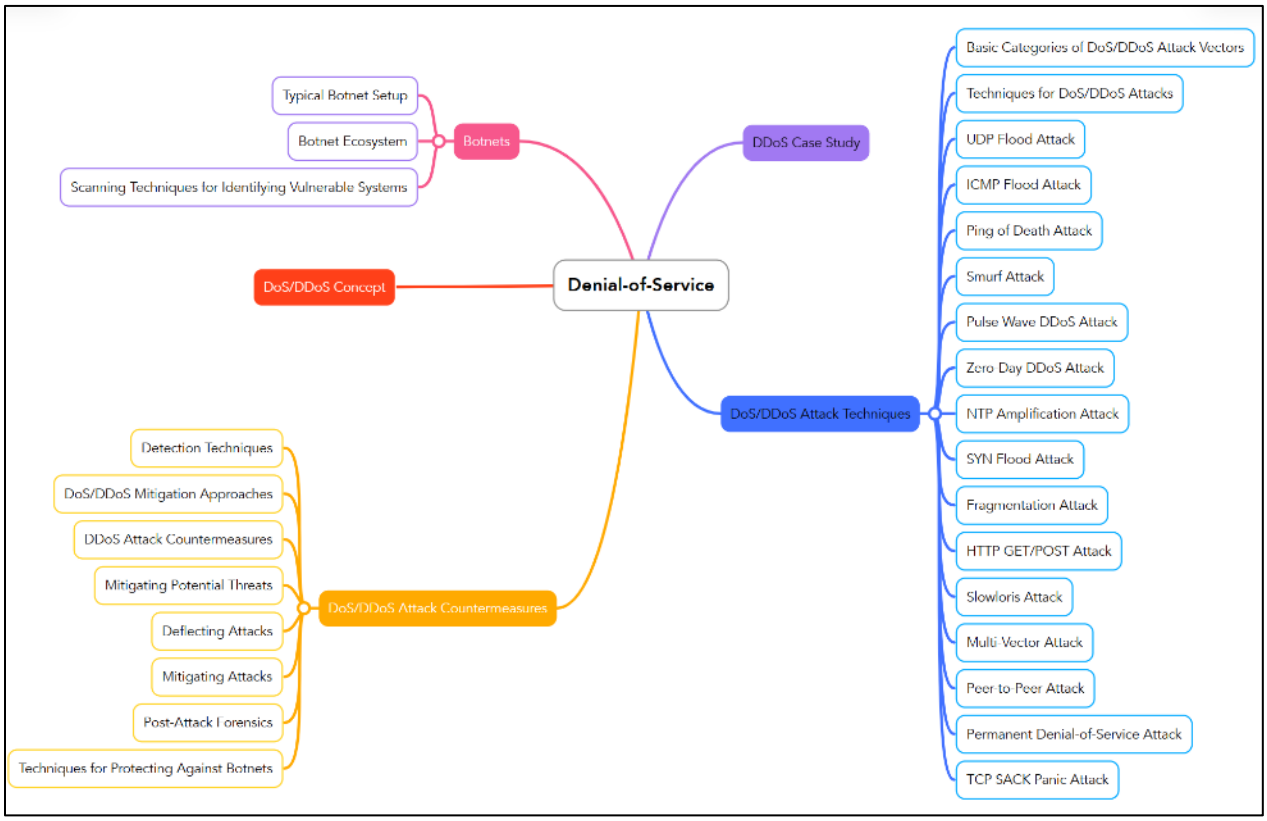

Figure 10-40: Mind Map

Practice Questions

1. What distinguishes a DoS attack from a DDoS attack?

A. DoS targets multiple systems, while DDoS targets a single system

B. DoS uses one source, DDoS uses many

C. DoS uses botnets, while DDoS does not

D. DoS attacks are legitimate traffic, while DDoS attacks use fake traffic

2. What are botnets commonly used for?

A. Performing malicious activities

B. Automating administrative tasks

C. Developing secure software

D. Enhancing network security

3. How do hackers commonly promote botnets for download?

A. Through legitimate software updates
B. By advertising on blogs, social media, and search engines
C. By offering free antivirus software
D. Through phone calls to unsuspecting users

4. Why are Android devices a popular target for botnet creation?
A. They are expensive devices
B. They have strong security measures
C. They are vulnerable to malware like Trojans and bots
D. They are rarely used for internet access

5. What is a key characteristic of a pulse wave DDoS attack?
A. It relies on amplification techniques
B. It delivers bursts of traffic in repetitive intervals
C. It only targets mobile devices
D. Basic firewalls easily mitigate it.

6. What does a SYN flood attack exploit in a system?
A. The server's ability to authenticate packets
B. The DNS query resolution process
C. The TCP three-way handshake process
D. The routing table's capacity

7. What type of attack does the Slowloris tool execute?
A. Layer-3 volumetric attacks
B. Layer-4 SYN flood attacks
C. Layer-7 HTTP connection attacks
D. Fragmentation attacks

8. Which attack specifically targets hardware components, causing irreversible damage?
A. Multi-vector attack
B. Permanent Denial-of-Service (PDoS) attack
C. HTTP POST flood attack

D. Fragmentation attack

9. What vulnerability does a TCP SACK panic attack exploit?
A. The server's firewall misconfiguration
B. An integer overflow in the Linux socket buffer
C. A misconfigured TCP three-way handshake process
D. Insufficient SYN/ACK packet handling

10. How does a random recursive GET flood attack primarily operate?
A. By sending malformed HTTP packets to the server
B. By generating multiple SYN packets to overwhelm the server
C. By simulating navigation through web pages using random numbers
D. By targeting UDP-based protocols with large packet sizes

11. What is a common method attackers use in peer-to-peer attacks?
A. Botnets to overwhelm a target system
B. Redirecting peer-to-peer network users to a victim's site
C. Exploiting UDP protocols to execute volumetric attacks
D. Sending incomplete TCP packets to the server

12. What is the primary goal of a multi-vector DDoS attack?
A. To exploit a single vulnerability in a system
B. To bypass firewalls using spoofed traffic
C. To simultaneously utilize multiple attack methods to overwhelm a target
D. To exhaust bandwidth using only volumetric attacks

13. Which of the following is a variant of the SYN flood attack?
A. Peer-to-Peer attack
B. HTTP GET/POST attack
C. TCP SACK Panic attack
D. Fragmentation attack

14. What is a SYN flood attack?

A. A method used to send overwhelming amounts of data to a server

B. A technique that exploits the TCP three-way handshake by sending multiple SYN requests using spoofed IP addresses

C. A tactic that disrupts web servers by sending excessive HTTP requests

D. An attack aimed at overwhelming a database server with high-speed queries

15. Which technique is used to prevent SYN flood attacks?

A. Installing firewalls to block unsolicited packets

B. Using SYN cookies to validate incomplete connections

C. Disabling all incoming connections

D. Limiting bandwidth usage to a single user

16. What is the primary characteristic of a Distributed Reflection Denial-of-Service (DRDoS) attack?

A. It uses direct flooding from multiple sources to attack a target

B. It uses intermediary victims to send spoofed packets to reflectors, overwhelming the target

C. It involves encrypting the attack traffic to evade detection

D. It targets only the application layer

17. Which protocol is recommended to disable as a countermeasure against DRDoS attacks?

A. Remote Procedure Call (RPC)

B. Simple Network Management Protocol (SNMP)

C. Character Generator Protocol (CHARGEN)

D. File Transfer Protocol (FTP)

18. Which is a recommended countermeasure to mitigate ransom DDoS (RDDoS) attacks?

A. Increasing server bandwidth

B. Deploying robust DDoS protection solutions

C. Paying the ransom to avoid the attack

D. Installing an IDS system to detect traffic spikes

19. What is a feature of the UltraDDOS-v2 attack tool?

A. It provides a command-line interface for advanced attack configurations

B. It includes a graphical user interface for easier attack setup and monitoring

C. It targets only the UDP protocol for flooding

D. It can perform attacks solely on application-layer protocols

20. Which strategy helps identify and neutralize handlers in a DDoS attack?

A. Network traffic analysis

B. Wavelet-based signal analysis

C. Packet traceback

D. Egress filtering

21. What method involves examining network traffic based on packet header information to detect DoS/DDoS attacks?

A. Sequential Change-Point Detection

B. Egress Filtering

C. Wavelet-Based Signal Analysis

D. Activity Profiling

22. Which method involves preventing unauthorized or harmful traffic from leaving the network?

A. Egress Filtering

B. Ingress Filtering

C. Load Balancing

D. Event Log Analysis

23. What is the primary challenge in detecting DoS/DDoS attacks?

A. Identifying legitimate traffic

B. Filtering out fraudulent traffic from legitimate sources

C. Recognizing network worms

D. Implementing a firewall

24. What is the primary purpose of "Honeypots" in DDoS mitigation?

A. To absorb malicious traffic during an attack

B. To attract and monitor DDoS attackers

C. To distribute DDoS attack traffic across multiple servers

D. To provide false data that misleads attackers

25. What is "Post-Attack Forensics" primarily used for?

A. To recover lost data during a DDoS attack

B. To analyze DDoS traffic patterns and identify attack sources

C. To prevent future DDoS attacks through advanced security systems

D. To isolate network traffic from legitimate users

Chapter 10: Denial-of-Service

1. **Answer: B**

Explanation: A DoS attack typically originates from a single source, while a DDoS attack uses multiple compromised systems (botnets) to generate traffic, making it harder to mitigate.

2. **Answer: A**

Explanation: Botnets are networks of compromised systems often used by attackers for malicious purposes, including DDoS attacks, spamming, and data theft.

3. **Answer: B**

Explanation: Hackers use platforms like blogs, search engines, and social media to disseminate advertisements containing botnet download links, often employing deceptive tactics like fake security alerts.

4. **Answer: C**

Explanation: Android devices, especially those using third-party app stores, are highly susceptible to malware, making them prime targets for attackers to expand their botnet networks.

5. **Answer: B**

Explanation: Pulse wave DDoS attacks generate high bursts of traffic at periodic intervals, overwhelming the target's bandwidth and making recovery challenging.

6. **Answer: C**

Explanation: A SYN flood attack takes advantage of the three-way handshake by sending multiple SYN requests without completing the connection, which overwhelms the server's resources and leaves connections in a pending state.

7. **Answer: C**

Explanation: Slowloris is designed to perform a Layer-7 attack by sending incomplete HTTP requests, causing the server to keep connections open and eventually exhausting its resources.

8. **Answer: B**

Explanation: A PDoS attack exploits hardware vulnerabilities, often through malicious firmware updates, to permanently damage the targeted device, necessitating replacement or reinstallation.

9. **Answer: B**

Explanation: TCP SACK panic attacks exploit a vulnerability in the Linux Socket Buffer, where an overflow occurs when the buffer exceeds its segment capacity, leading to kernel panic.

10. **Answer: C**

Explanation: In a random recursive GET flood attack, attackers simulate legitimate browsing behavior using random numbers to generate GET requests, thereby consuming server resources.

11. **Answer: B**

Explanation: In a peer-to-peer attack, attackers manipulate peer-to-peer protocols to redirect large numbers of users to a victim's website, causing significant strain on its resources.

12. **Answer: C**

Explanation: Multi-vector DDoS attacks combine volumetric, protocol, and application-layer methods to confuse defenses and exhaust resources, making mitigation more challenging.

13. **Answer: C**

Explanation: TCP SACK Panic attack is a variant of SYN flood attacks that targets vulnerabilities within the Linux kernel related to Selective Acknowledgment (SACK) and socket buffer overflows.

14**. Answer: B**

Explanation: A SYN flood attack exploits the TCP three-way handshake by sending numerous SYN requests with fake IP addresses, overwhelming the target server and exhausting its resources.

15. **Answer: B**

Explanation: SYN cookies are a technique used to mitigate SYN flood attacks by validating requests without relying on stateful connection tracking, thus minimizing the resource usage on the server.

16. **Answer: B**

Explanation: DRDoS attacks rely on intermediary victims (zombies) sending spoofed packets to reflectors, which in turn flood the primary target with traffic, making it challenging to trace the true attacker.

17. **Answer: C**

Explanation: Disabling the Character Generator Protocol (CHARGEN) helps mitigate DRDoS attacks, as it is one of the protocols commonly exploited by attackers for reflection-based attacks.

18. **Answer: B**

Explanation: The best way to counter RDDoS attacks is by deploying strong DDoS protection services, which can help to absorb and mitigate attack traffic rather than paying the ransom.

19. **Answer: B**

Explanation: UltraDDOS-v2 provides a user-friendly graphical interface, allowing users to easily specify target IP addresses, ports, and packet volumes for DDoS attacks.

20. **Answer: A**

Explanation: Identifying and neutralizing handlers involves analyzing network traffic to spot the intermediaries (handlers) who facilitate DDoS attacks. By tracing the traffic between handlers and agents, administrators can locate and neutralize the handlers to disrupt the attack.

21. **Answer: D**

Explanation: Activity profiling is based on the analysis of network flow clusters and packet rate patterns to identify abnormalities indicative of DoS/DDoS attacks.

22. **Answer: A**

Explanation: Egress filtering ensures that outgoing traffic from the network adheres to specific criteria, preventing malicious or unauthorized packets from leaving the network.

23. **Answer: B**

Explanation: Detecting DoS/DDoS attacks is challenging because it is difficult to distinguish fraudulent traffic from legitimate traffic due to the sheer volume of data. Current detection methods focus on identifying deviations in traffic patterns, but filtering malicious traffic from legitimate user traffic remains a significant issue.

24. **Answer: D**

Explanation: Identifying and neutralizing handlers involves analyzing network traffic to spot the intermediaries (handlers) who facilitate DDoS attacks. By tracing the traffic between handlers and agents, administrators can locate and neutralize the handlers to disrupt the attack.

25. **Answer: B**

Explanation: Honeypots are systems designed with minimal security to attract attackers. They allow security teams to collect information about the attackers' techniques and tools. This helps in monitoring attacks and improving the overall defense against future threats.