Module 12
Denial of Service

Ansh Bhawnani

DoS/DDoS Concepts

Module 12

DoS/DDoS Concepts

What is a Denial-of-Service Attack?

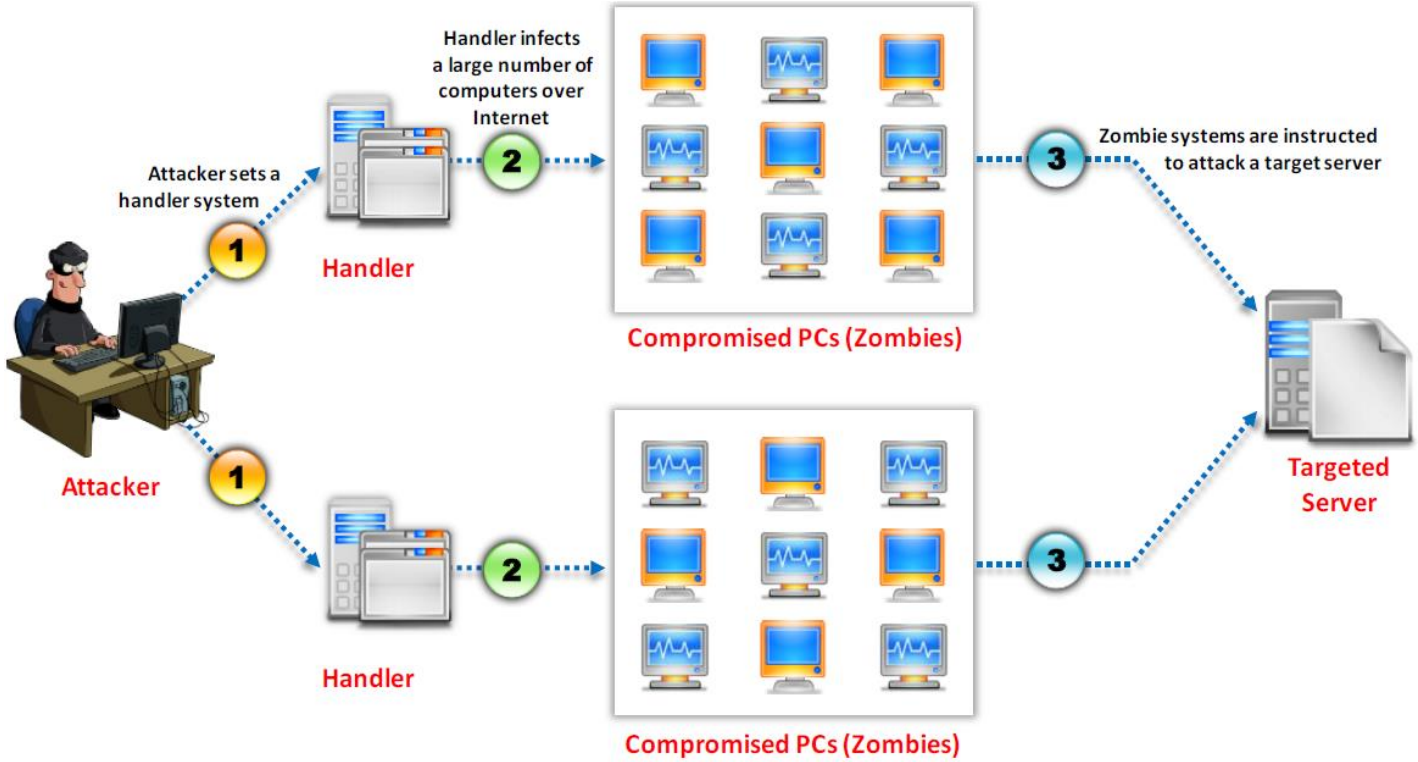
- Denial of Service (DoS) is an attack on a computer or network that reduces, restricts or prevents accessibility of system resources to its legitimate users.
- In a DoS attack, attackers flood a victim system with non-legitimate service requests or traffic to overload its resources.
- DoS attack leads to unavailability of a particular website and slow network performance.

DoS/DDoS Concepts

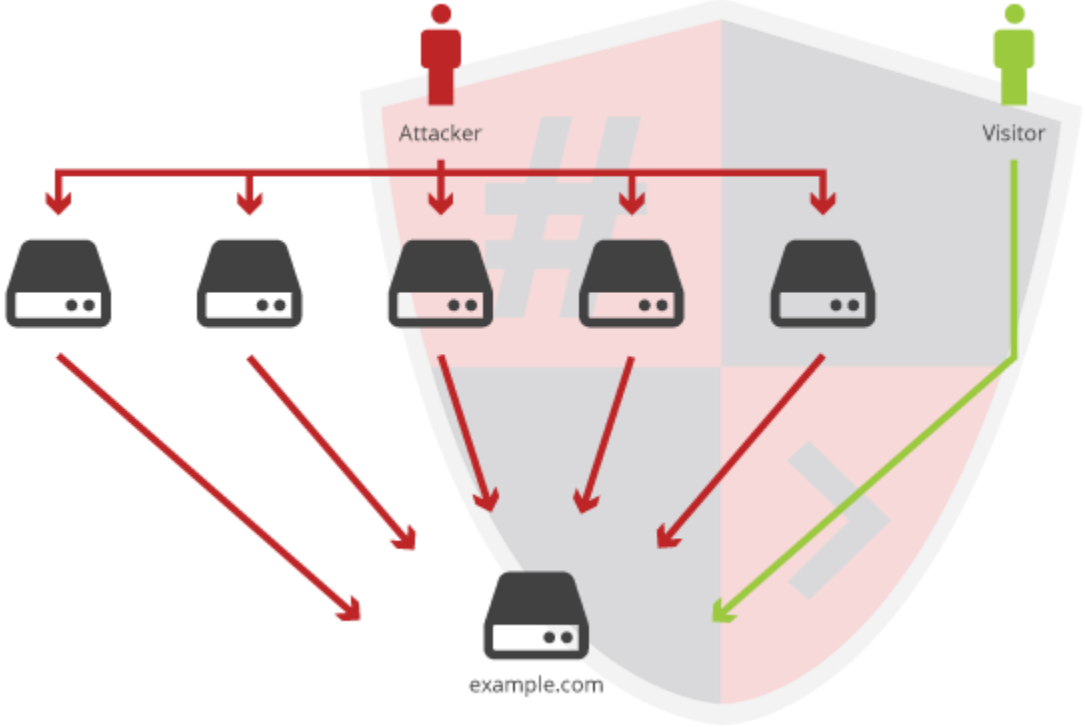
What are Distributed Denial of Service Attacks?

- A distributed denial-of-service (DDoS) attack involves a multitude of compromised systems attacking a single target, thereby causing denial of service for users of the targeted system.
- To launch a DDoS attack, an attacker uses botnets and attacks a single system.

DoS/DDoS Concepts



DoS/DDoS Concepts



DoS/DDoS Attacks Techniques

Module 12

DoS/DDoS Attacks Techniques

Basic Categories of DoS/DDoS Attack Vectors

- **Volumetric Attacks**: Consumes the bandwidth of target network or service.
- **Fragmentation Attacks**: Overwhelms target's ability of re-assembling the fragmented packets.
- **TCP State-Exhaustion Attacks**: Consumes the connection state tables present in the network infrastructure components such as load-balancers, firewalls, and application servers.
- **Application Layer Attacks**: Consumes the application resources or service thereby making it unavailable to other legitimate users.

DoS/DDoS Attacks Techniques

DoS/DDoS Attack Techniques

- Bandwidth Attacks and Service Request Floods
- SYN Flooding Attack
- ICMP Flood Attack
- Peer-to-Peer Attacks
- Application-Level Flood Attacks
- Permanent Denial-of-Service Attack
- Distributed Reflection Denial of Service (DrDoS)

DoS/DDoS Attacks Techniques

Bandwidth Attacks

- When a DDoS attack is launched, flooding a network, it can cause network equipment such as switches and routers to be overwhelmed due to the significant statistical change in the network traffic.
- Attackers use botnets and carry out DDoS attacks by flooding the network with ICMP ECHO packets.
- Basically, all bandwidths is used and no bandwidth remains for legitimate use.

DoS/DDoS Attacks Techniques

Service Request Floods

- An attacker or group of zombies attempts to exhaust server resources by setting up and tearing down TCP connections.
- Service request flood attacks flood servers with a high rate of connections from a valid source.
- It initiates a request on every connection.

DoS/DDoS Attacks Techniques

SYN Attack

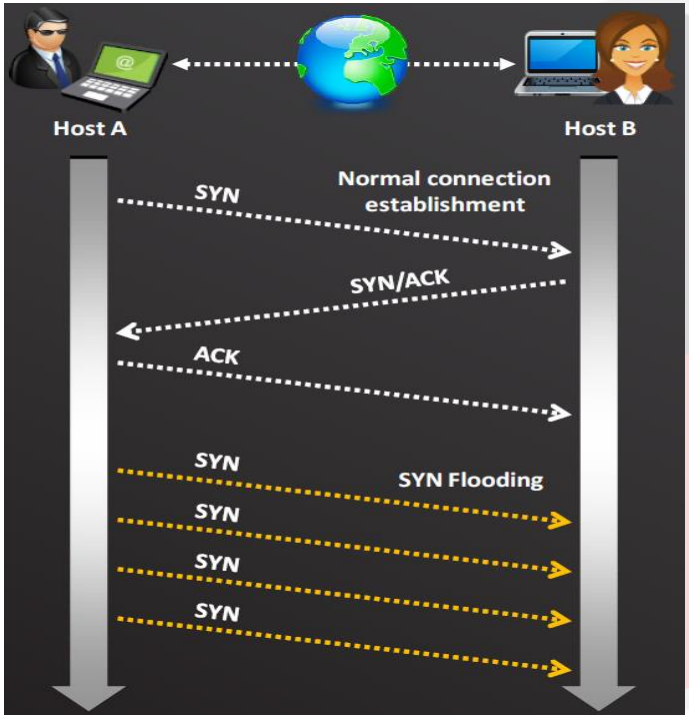
- The attacker sends a large number of SYN request to target server (victim) with fake source IP addresses.
- The target machine sends back a SYN/ACK in response to the request and waits for the ACK to complete the session setup.
- The target machine does not get the response because the source address is fake.

DoS/DDoS Attacks Techniques

SYN Flooding (SlowLoris)

- SYN Flooding takes advantage of a flaw in how most hosts implement the TCP three-way handshake.
- When Host B receives the SYN request from A, it must keep track of the partially-opened connection in a "listen queue" for at least 75 seconds.
- A malicious host can exploit the small size of the listen queue by sending multiple SYN requests the a host, but never replying to the SYN/ACK.
- The victim's listen queue is quickly filled up.
- The ability of holding up each incomplete connection for 75 seconds can be cumulatively used as a Denial of Service attack.

DoS/DDoS Attacks Techniques

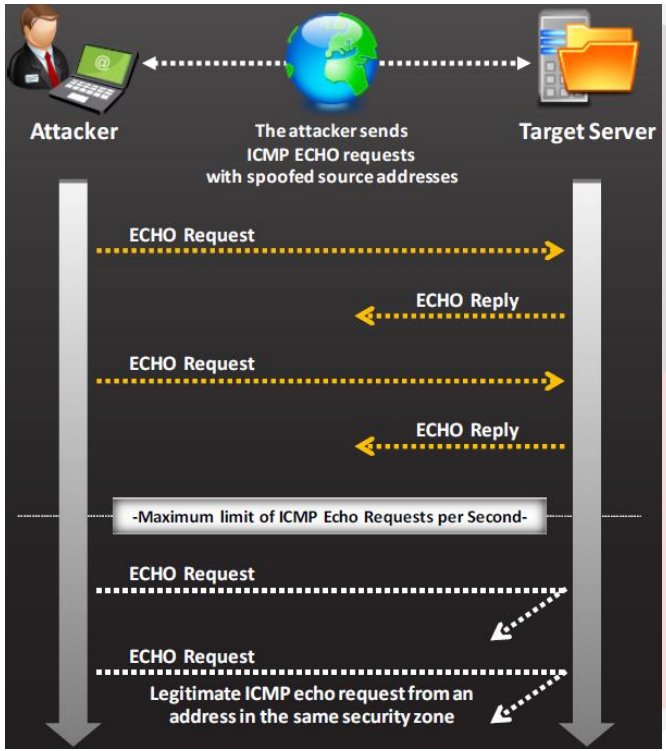


DoS/DDoS Attacks Techniques

ICMP Flood Attack

- ICMP flood attack is a type DoS attack in which perpetrators send a large number of ICMP packets directly or through reflection networks to victims causing it to be overwhelmed and subsequently stop responding to legitimate TCP/IP requests.
- To protect against ICMP flood attack, set a threshold limit that when exceeds invokes the ICMP flood attack protection feature.

DoS/DDoS Attacks Techniques

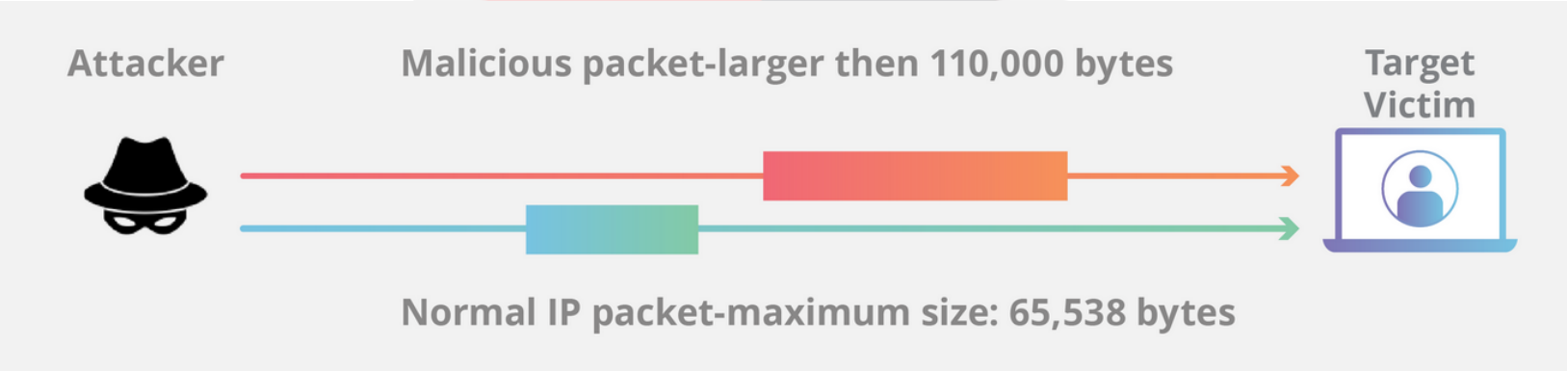


DoS/DDoS Attacks Techniques

Ping of Death attack

- The attacker aims to disrupt a targeted machine by sending a packet larger than the maximum allowable size, causing the target machine to freeze or crash.
- IP4 ping packets are much larger, and can be as large as the maximum allowable packet size of 65,535 bytes. Some TCP/IP systems were never designed to handle packets larger than the maximum, making them vulnerable to packets above that size.

DoS/DDoS Attacks Techniques

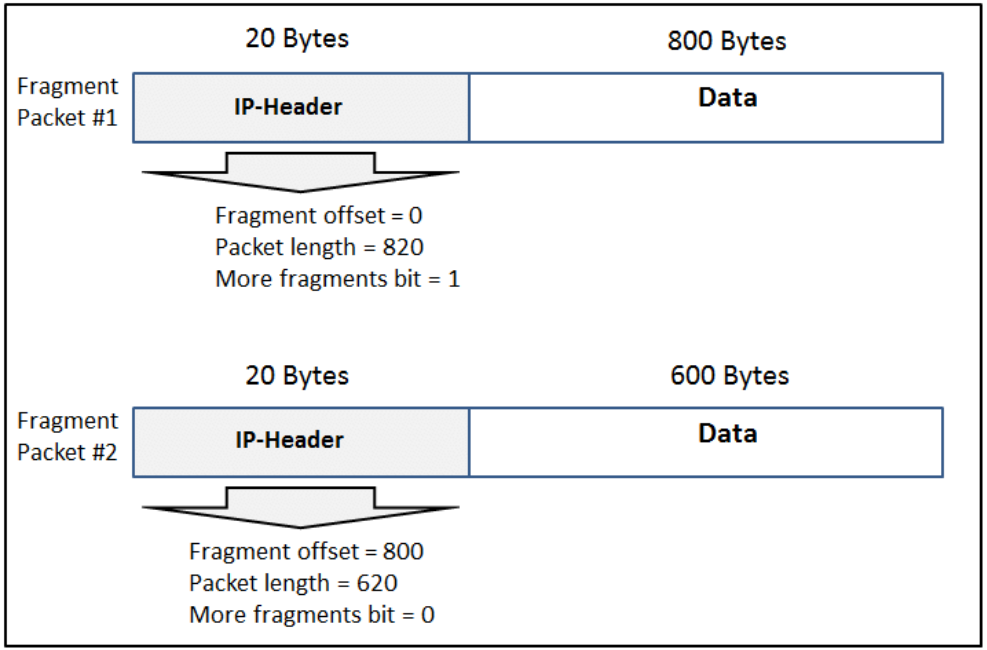


DoS/DDoS Attacks Techniques

Teardrop Attack

- Targets TCP/IP reassembly mechanisms, preventing them from putting together fragmented data packets. As a result, the data packets overlap and quickly overwhelm the victim's servers, causing them to fail.
- Teardrop attacks are a result of an OS vulnerability common in older versions of Windows, including 3.1, 95 and NT, resurfaced in Windows 7 and Vista.

DoS/DDoS Attacks Techniques

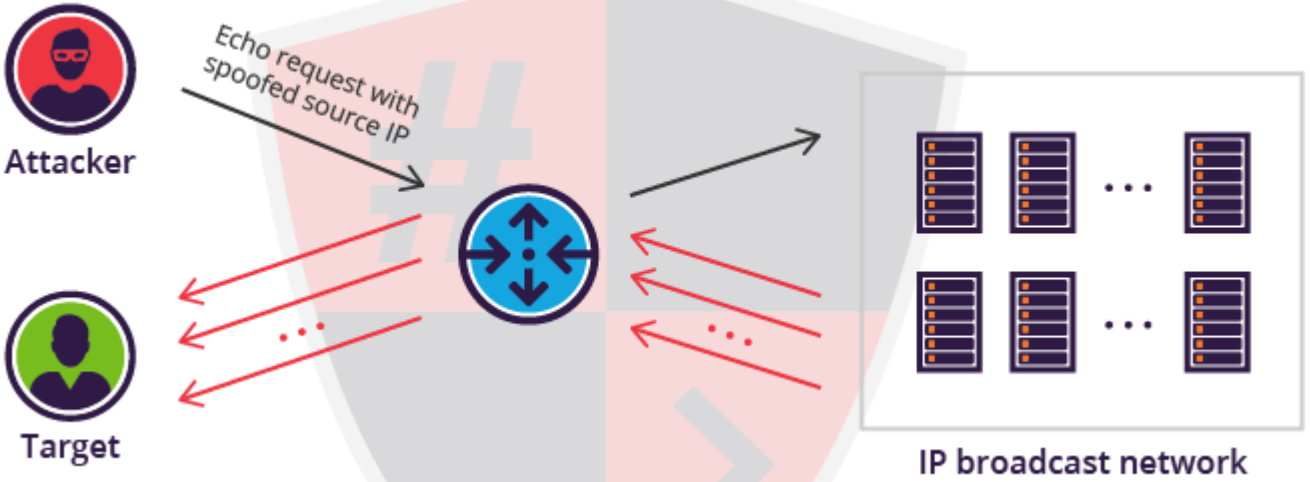


DoS/DDoS Attacks Techniques

Smurf Attack

- Distributed denial-of-service attack in which large numbers of (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP broadcast address.
- The response from all the machines will be reflected towards to the victim’s machine in exceptionally large numbers, causing it to freeze or hang (multiplied upto 255 times).

DoS/DDoS Attacks Techniques



DoS/DDoS Attacks Techniques

Peer-to-Peer Attacks

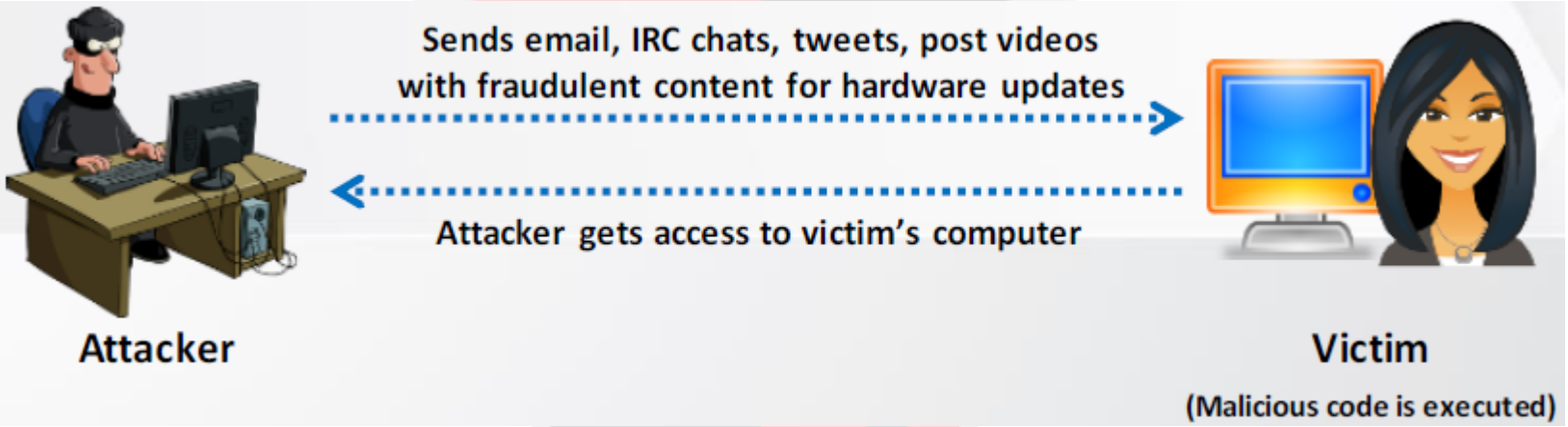
- Using peer-to-peer attacks, attackers instruct clients of peer-to-peer file sharing hubs to disconnect from their peer-to-peer network and to connect to the victim's fake website.
- Attackers exploit flaws found in the network using DC++ (Direct Connect) protocol, that is used for sharing all types of files between instant messaging clients.
- Using this method, attackers launch massive denial-of-service attacks and compromise websites.

DoS/DDoS Attacks Techniques

Permanent Denial-of-Service (PDoS) Attack

- **Phlashing**: Permanent DoS, also known as phlashing, refers to attacks that cause irreversible damage to system hardware.
- **Sabotage**: Unlike other DoS attacks, it sabotages the system hardware, requiring the victim to replace or reinstall the hardware.
- **Bricking a system**: This attack is carried out using a method known as "bricking a system“. Using this method, attackers send fraudulent hardware updates to the victims.

DoS/DDoS Attacks Techniques



Application Level DoS/DDoS attacks

Module 12

DoS/DDoS Attacks Techniques

Application-Level Flood Attacks

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

DoS/DDoS Attacks Techniques

- **Using application-level flood attacks, attackers attempts to:**
  - Flood web applications to legitimate user traffic.
  - Disrupt service to a specific system or person, for example, blocking a user's access by repeating invalid login attempts.
  - Jam the application-database connection by crafting malicious SQL queries.

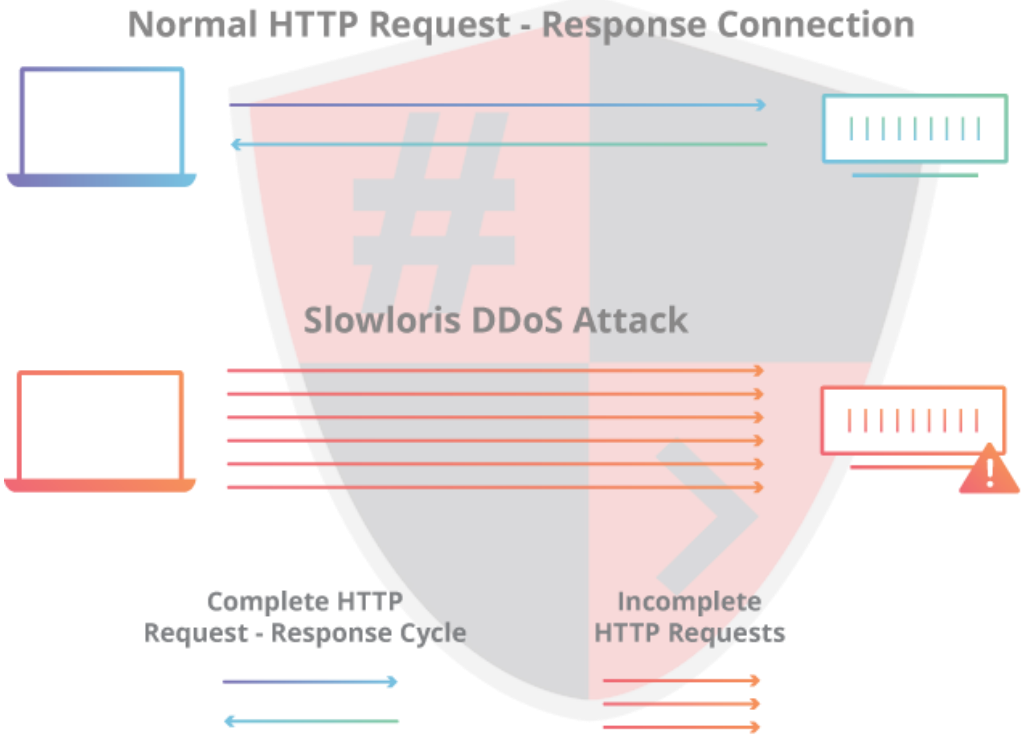
1. SlowLoris

DoS/DDoS Attacks Techniques

SlowLoris attack

- Slowloris is a denial-of-service attack program which allows an attacker to overwhelm a targeted server by opening and maintaining many simultaneous HTTP connections between the attacker and the target.
- It falls in the category of attacks known as “low and slow” attacks.
- The targeted server will only have so many threads available to handle concurrent connections. Each server thread will attempt to stay alive while waiting for the slow request to complete, which never occurs.
- When the server’s maximum possible connections has been exceeded, each additional connection will not be answered and denial-of-service will occur.

DoS/DDoS Attacks Techniques



DoS/DDoS Attacks Techniques

A Slowloris attack occurs in 4 steps:

- The attacker first opens multiple connections to the targeted server by sending multiple partial HTTP request headers.
- The target opens a thread for each incoming request, with the intent of closing the thread once the connection is completed. In order to be efficient, if a connection takes too long, the server will timeout the exceedingly long connection, freeing the thread up for the next request.

DoS/DDoS Attacks Techniques

- To prevent the target from timing out the connections, the attacker periodically sends partial request headers to the target in order to keep the request alive. In essence saying, **“I’m still here! I’m just slow, please wait for me**.”
- The targeted server is never able to release any of the open partial connections while waiting for the termination of the request. Once all available threads are in use, the server will be unable to respond to additional requests made from regular traffic, resulting in denial-of-service.

2. Random Access Memory (RAM)

Module 12

DoS/DDoS Attacks Techniques

Recursion

- It refers to a procedure that causes itself to repeat over and over again.
- In most cases, this is a controlled process and a valid technique in programming.
- In the case of L7 DoS, it's the result of a small set of instructions whose execution prompts vulnerable applications to enter a resource-intensive loop, with the specific purpose of exhausting their resources.

DoS/DDoS Attacks Techniques

What to look out for

Example of PHP code:
include('current_file_name.php');

Where it is found

This kind of vulnerability can be found in places where a traditional Local File Inclusion (LFI)

DoS/DDoS Attacks Techniques

Zip bombs

- In the early 2000s, ZIP bombs were emailed to unsuspecting victims in order to crash their personal computers or mail servers.
- Ironically, this was often the fault of the system's antivirus program's automated extraction of the archive (in order to scan it), not that of the user opening it. Now, most antivirus vendors would either detect ZIP bombs or avoid extracting them completely.

DoS/DDoS Attacks Techniques

- Briefly, some file compression algorithms work by replacing recurring patterns in the file with short references to a single occurrence of the pattern. Let's say that instead of writing '**AAAAAAAAAAAAAAAA**', you could write '**1-16-A**' to display the character 'A' sixteen times at position 1. Replace '16' with '999999999', and you'll understand why a relatively small file can consume all the RAM or disk space once extracted.
- One famous example of a ZIP bomb is **42.zip,** which is just 42 kb in size, but increases to 4.5 petabytes (approximately the size of 1.125 billion MP3 files).

DoS/DDoS Attacks Techniques

Where it is found

Web applications that allow you to upload compressed files, and extract the content for you, might be susceptible to such an attack, particularly if the application (or or the library that handles the decompression) fails to conduct a proper inspection of the deflated file.

DoS/DDoS Attacks Techniques

Deserialization Vulnerabilities

- Deserialization is a delicate topic and you should generally not deserialize user supplied input using functions that are not explicitly recommended as safe alternative to raw deserialization functions.
- It might be possible to pass a string to a deserialization function that instructs the parser to allocate large chunks of memory (for example by using repeating nested array definitions as seen in the linked paper about various PHP vulnerabilities).
- A wide range of programming languages with a similar functionality, in addition to PHP, can be vulnerable.

DoS/DDoS Attacks Techniques

Where it is found

Deserialization vulnerabilities may be found everywhere user input is accepted. Most of the time you can see where serialized strings are accepted by using the application normally and intercepting the traffic with a tool like Fiddler.

DoS/DDoS Attacks Techniques

Manipulating File Headers to Allocate Large Memory Chunks

- The **HackerOne** example illustrates a hacker manipulating file headers to allocate large memory chunks.
- Using a 260px * 260px jpg file, the researcher manipulated the file header in order to make it appear as if the image was 64250px * 64250px in size. This relatively small file eventually led to a DoS condition on HackerOne, and apparently on the researcher's local image viewer.
- This happened because the application allocated a large amount of memory, ran out of RAM, swapped to disk and eventually denied service altogether.

DoS/DDoS Attacks Techniques

Where it is found

This vulnerability might be found in places where computation is performed on an input file, and where the size of the file is saved in its header. This might include images and video files, and other file formats.

3. Central Processing Unit (CPU)

Module 12

DoS/DDoS Attacks Techniques

reDoS

- reDoS (Regular Expression Denial of Service) was put under the spotlight in 2016 when it caused stackoverflow.com to go offline for just over 30 minutes.
- It wasn't the fault of an attacker, but a user who included 20,000 whitespace characters in a code snippet.
- According to the write-up, the regular expression was written in such a way that it forced the system to check the 20,000 character string in 200,010,000 steps (20,000 + 19,000, + … + 2 + 1).

DoS/DDoS Attacks Techniques

Where it is found

If a web application allows you to input your own regex code, it might be possible to execute the above-mentioned attack. In older versions of PHP, it might even lead to remote code execution.

DoS/DDoS Attacks Techniques

SQL Injection Wildcard Attack

- An SQL injection wildcard attack works in a similar way to a plain reDoS.
- The key difference is that it doesn't just use the usual regular expression syntax, but employs so-called 'wildcards' that are used by databases to find data matching a specific description.
- These attacks can either be carried out using an (otherwise not vulnerable) search functionality, or via an attack vector, where it's possible to execute SQL statements, for example with an existing SQL injection vulnerability.

DoS/DDoS Attacks Techniques

Where it is found

Due to the nature of the vulnerability and the affected SQL functions, it can often be found in search functionality. To learn more about how such attacks are conducted, see the linked paper.

DoS/DDoS Attacks Techniques

Fork Bombs

- Fork bombs are processes that duplicate themselves over and over again until they use up all of the system's resources. Both the CPU and the process table are affected.
- They acquired their name from the fork system call that they use. Perhaps the most commonly-known fork bomb is the following shell command: **:(){ :|:& };:**
- This shows that fork bombs use recursion as the : function calls itself over and over again. Fork bombs are rarely used in web application attacks.

DoS/DDoS Attacks Techniques

Where it is found

This attack would be conducted in a sandboxed environment that allows code execution of some sort, without giving an attacker access to sensitive data. Otherwise an attacker might decide to use the code execution for malicious purposes that are worse than a Denial of Service attack.

DoS/DDoS Attacks Techniques

Abusing Password Hashing Functions

- Modern password hashing functions are designed to be ineffective, which is achieved by so-called 'key stretching'.
- They need a lot of time and resources to return the desired output. This is intentional because it slows down attackers that are trying to find the passwords belonging to those hashes.
- This property distinguishes these algorithms from the ones used in other kinds of hashing functions. These are generally designed to quickly return checksums for large files.

DoS/DDoS Attacks Techniques

Where it is found

Attackers could abuse this fact to achieve a DoS attack, if they submitted a huge amount of long passwords to the hashing function. Depending on the cost factor and server hardware, this could easily lead to a DoS.

4. Disk Space

Module 12

DoS/DDoS Attacks Techniques

Uploading Large Files

- Arguably the most obvious way to fill a system with data is by uploading large files to the server.
- If the application doesn't apply proper rate-limiting and size checks for its file upload functionality, an attacker can upload random junk data to the system until it can no longer store any more data.
- This either makes the file upload functionality fail for legitimate users, or can make the entire system unstable.

DoS/DDoS Attacks Techniques

Where it is found

Profile picture upload functionality, while ubiquitous, is fortunately unsuitable for this type of attack because previous uploads are deleted once a user uploads a new image. Instead, this can be achieved by uploading files in private messages or in bug reports or help desk applications.

DoS/DDoS Attacks Techniques

Arbitrary File Deletion

- The deletion of arbitrary files is a completely different DoS approach. Using an arbitrary file deletion vulnerability, an attacker can remove data that is necessary for the application in order to work correctly.
- This may include removing configuration files or even script code in order to deny service to legitimate users.

Where it is found

Where to find such a vulnerability is highly application-specific. But it often involves directory traversal.

5. Exhaust Allocated Resources for a Single User

Module 12

DoS/DDoS Attacks Techniques

Email Bomb

- Users are regularly allocated a small amount of space for their inbox.
- The goal of an Email Bomb is to flood a user's inbox to the point where all available space is exhausted, and subsequent (legitimate) emails bounce.

DoS/DDoS Attacks Techniques

Where it is found

Attackers can abuse this flaw by sending a moderately large amount of emails with large attachments. After a short time, the mailbox is full and new emails are rejected. While it should be easy to fill a victim's inbox if space is tight, there is an attack called List Linking that addresses targets with larger inboxes. An attacker registers the victim for various, high-frequency mailing lists and lets them spam the inbox.

DoS/DDoS Attacks Techniques

Free Website Restrictions

- Some web hosts allow only a certain amount of requests per day for users on free subscriptions. If the amount of requests exceeds the maximum limit, the page becomes unavailable for a certain amount of time, except if the user pays for a subscription.

Where it is found

It is relatively easy to trigger this maximum limit by querying the site in a continuous loop, using a tool like cURL. There are only two lines needed in order to create a valid HTTP 1.1 request.

DoS/DDoS Attacks Techniques

Cash Overflow

- A similar approach is called Cash Overflow. Instead of targeting disk space, RAM or the CPU, the attack aims to raise the bill for a service up to the point where it exceeds the allocated amount of money.
- Should the owner of the website be unable to pay the bill or if automatic payment fails, the service will be terminated – effectively leading to DoS. This can happen if an external service is used that bills the user a certain amount of money per request.

6. Logic-Based Denial of Service

Module 12

DoS/DDoS Attacks Techniques

X-Forwarded-For

- If the application incorrectly uses headers like X-Forwarded-For in order to determine users' IP addresses.
- It's easy to forget that this flawed implementation also opens the door for a DoS attack, if the IP address of a legitimate user is used instead of a random one for example.
- Attackers may constantly trigger rate limiting, with an X-Forwarded-For header containing the victims' IP address. If victims can't mask or change their IP address, they are denied service for the duration of the attack.

DoS/DDoS Attacks Techniques

Where it is found

This flaw can be found on any application protected by a web application firewall (WAF), or any application that applies rate limiting as long as either of these measures can be bypassed using X-Forwarded-For.

DoS/DDoS Attacks Techniques

Web Application Firewalls

- Many web application firewalls can be configured to block users that send malicious requests, for a certain amount of time.
- Those requests may contain specific, special characters like backticks and single quotes or blocked keywords such as script and passwd. An attacker can set up a page that will send such requests to a WAF-protected website, or in other words, trigger the DoS condition through CSRF.
- Once it sees the request coming from the victim's IP, it will automatically block it for a certain amount of time. The same works if the attacker is able to set a cookie with a blocked keyword.

DoS/DDoS Attacks Techniques

Where it is found

This can be found wherever a WAF is protecting the application and users are blocked in the event of malicious keyword detection.

DoS/DDoS Attacks Techniques

Wasting the Available Password Attempts

- Preventing attackers from bruteforcing the credentials of legitimate users is difficult. Often this problem is solved using a captcha. But sometimes developers resort to blocking the account after a certain amount of wrong login attempts.
- If an attacker wastes all of the login attempts for a specific user, either accidentally while brute forcing or on purpose, the affected user will be denied access as well.

DoS/DDoS Attacks Techniques

Where it is found

This vulnerability can arise wherever there is a limited amount of password attempts per user, rather than per IP address or session. Sometimes applications will send a link to the victim in order to unblock the account again. This should be tested to avoid false positives.

DoS/DDoS Attacks Techniques

Cookie Bombs

- If an application endpoint allows the generation a big amount of cookies (a cookie bomb) with different names, an attacker can instruct the victim's browser to store and send enough cookies in order to exceed the allowed request size.
- This will eventually lead to a denial of service condition that can only be fixed by deleting all the malicious cookies.

DoS/DDoS Attacks Techniques

Where it is found

As mentioned above, the application must have cookies with different names in order for this to work. The attack would be triggered via CSRF.

DoS/DDoS Attacks Techniques

Distributed Reflection Denial of Service (DRDoS)

- A distributed reflected denial of service attack (DRDoS), also known as spoofed attack, involves the use of multiple intermediary and secondary machines that contribute to the actual DDoS attack against the target machine or application.
- Attacker launches this attack by sending requests to the intermediary hosts, these requests are then redirected to the secondary machines which in turn reflects the attack traffic to the target.

DoS/DDoS Attacks Techniques

Advantage:

- The primary target seems to be directly attacked by the secondary victim, not the actual attacker.
- As multiple intermediary victim servers are used which results into increase in attack bandwidth.

Botnets

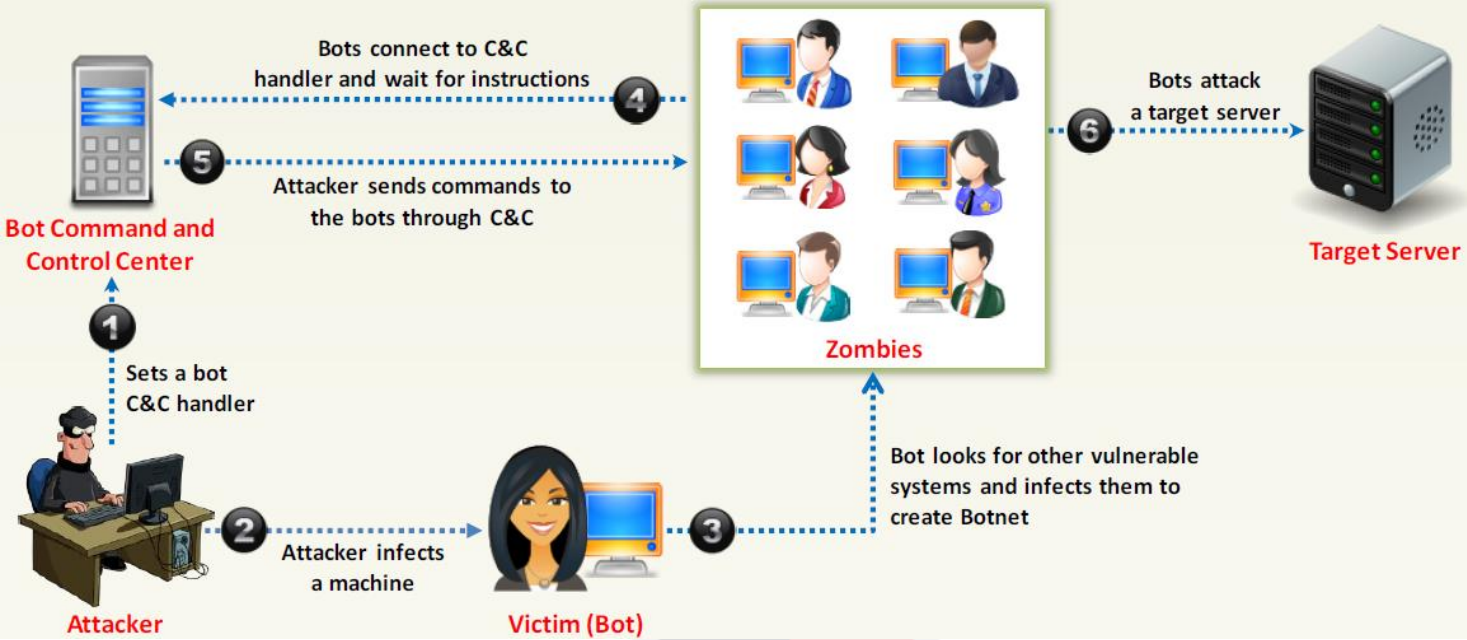
Module 12

Botnets

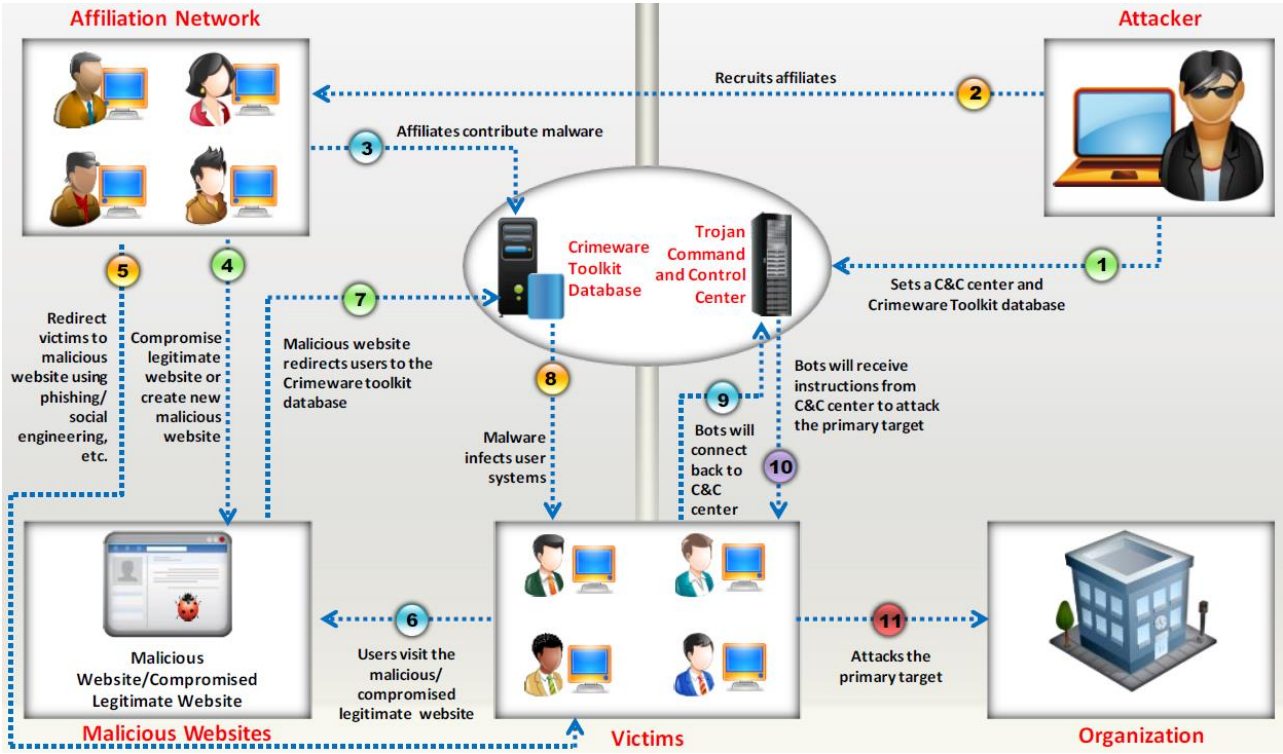
Botnets

- Bots are software applications that run automated tasks over the Internet and perform simple repetitive tasks, such as web spidering and search engine indexing.
- A botnet is a huge network of the compromised systems and can be used by an attacker to launch denial-of-service attacks.

Botnets


Bots connect to C&C handler and wait for instructions
4
5
Attacker sends commands to the bots through C&C
Bot Command and Control Center
1
Sets a bot C&C handler
Attacker
2
Attacker infects a machine
Victim (Bot)
3
Bot looks for other vulnerable systems and infects them to create Botnet
Zombies
6
Bots attack a target server
Target Server

Botnets


Affiliation Network
Attacker
Recruits affiliates
2
Affiliates contribute malware
3
Crimeware Toolkit Database
Trojan Command and Control Center
1
Sets a C&C center and Crimeware Toolkit database
5
4
7
Redirect victims to malicious website using phishing/ social engineering, etc.
Compromise legitimate website or create new malicious website
Malicious website redirects users to the Crimeware toolkit database
8
Malware infects user systems
9
Bots will connect back to C&C center
10
Bots will receive instructions from C&C center to attack the primary target
Malicious Website/Compromised Legitimate Website
6
Users visit the malicious/ compromised legitimate website
11
Attacks the primary target
Malicious Websites
Victims
Organization

Botnets

Scanning Methods for Finding Vulnerable Machines

- **Random Scanning:** The infected machine probes IP addresses randomly from target network IP range and checks for the vulnerability.
- **Hit-list Scanning:** Attacker first collects list of possible potentially vulnerable machines and then perform scanning to find vulnerable machine.
- **Topological Scanning**: It uses the information obtained on infected machine to find new vulnerable machines.
- **Local Subnet Scanning:** The infected machine looks for the new vulnerable machine in its own local network.
- **Permutation Scanning:** It uses pseudorandom permutation list of IP addresses to find new vulnerable machines.

Botnets

How Malicious Code Propagates?

- Attackers use three techniques to propagate malicious code to newly discovered vulnerable system:
  - **Central Source Propagation**: Attacker places attack toolkit on the central source and copy of the attack toolkit is transferred to the newly discovered vulnerable system.
  - **Back-chaining Propagation**: Attacker places attack toolkit on his/her system itself and copy of the attack toolkit is transferred to the newly discovered vulnerable system.
  - **Autonomous Propagation**: Attack toolkit is transferred at the time when the new vulnerable system is discovered.

Botnets

How Malicious Code Propagates?

- Attackers use three techniques to propagate malicious code to newly discovered vulnerable system:
  - **Central Source Propagation**: Attacker places attack toolkit on the central source and copy of the attack toolkit is transferred to the newly discovered vulnerable system.
  - **Back-chaining Propagation**: Attacker places attack toolkit on his/her system itself and copy of the attack toolkit is transferred to the newly discovered vulnerable system.
  - **Autonomous Propagation**: Attack toolkit is transferred at the time when the new vulnerable system is discovered.

DoS/DDoS Attack Detection

Module 12

Countermeasures

Detection Techniques

- Detection techniques are based on identifying and discriminating the illegitimate traffic increase and flash events from legitimate packet traffic.
- All detection techniques define an attack as an abnormal and noticeable deviation from a threshold of normal network traffic statistics.
  - **Activity Profiling**
  - **Wavelet-based Signal Analysis**
  - **Changepoint Detection**

Countermeasures

Activity Profiling

- An attack is indicated by:
  - An increase in activity levels among the network flow clusters.
  - An increase in the overall number of distinct clusters (DDoS attack)
- Activity profile is done based on the average packet rate for a network flow, which consists of consecutive packets with similar packet fields.
- Activity profile is obtained by monitoring the network packet's header information.

Countermeasures

Wavelet-based Signal Analysis

- Wavelet analysis describes an input signal in terms of spectral components.
- Wavelets provide for concurrent time and frequency description.
- Analyzing each spectral window's energy determines the presence of anomalies.
- Signal analysis determines the time at which certain frequency components are present.

Countermeasures

Sequential Change-Point Detection

- **Isolate Traffic**: Change-point detection algorithms isolate changes in network traffic statistics caused by attacks.
- **Filter Traffic**: The algorithms filter the target traffic data by address, port, or protocol and store the resultant flow as a time series.
- **Identify Attack**: Sequential change-point detection technique uses Cumulative Sum (Cusum) algorithm to identify and locate the DoS attacks; the algorithm calculates deviations in the actual versus expected local average in the traffic time series.
- **Identify Scan Activity**: This technique can also be used to identify the typical scanning activities of the network worms.

DoS/DDoS Attack Countermeasures

Module 12

Countermeasures

DoS/DDoS Countermeasure Strategies

- **Absorbing the Attack**:
  - Use additional capacity to absorb attack; it requires preplanning.
  - It requires additional resources.
- **Degrading Services**:
  - Identify critical services and stop non critical services.
- **Shutting Down the Services**:
  - Shut down all the services until the attack has subsided.

Countermeasures

Protect Secondary Victims

- Install anti-virus and anti-Trojan software and keep these up-to-date.
- Increase awareness of security issues and prevention techniques in all Internet users.
- Disable unnecessary services, uninstall unused applications, and scan all the files received from external sources.
- Properly configure and regularly update the built-in defensive mechanisms in the core hardware and software of the system.

Countermeasures

Detect and Neutralize Handlers

- **Network Traffic Analysis**: Analyze communication protocols and traffic patterns between handlers and clients or handlers and agent in order to identify the network nodes that might be infected by the handlers.
- **Neutralize Botnet Handlers**: There are usually few DDoS handlers deployed as compared to the number of agents. Neutralizing a few handlers can possibly render multiple agents useless, thus thwarting DDoS attacks.
- **Spoofed Source Address**: There is a decent probability that the spoofed source address of DDoS attack packets will not represent a valid source address of the definite sub-network.

Countermeasures

Detect Potential Attacks

- **Egress Filtering**: Scanning the packet headers of IP packets leaving a network. Egress filtering ensures that unauthorized or malicious traffic never leaves the internal network.
- **Ingress Filtering**: Protects from flooding attacks which originate from the valid prefixes (IP address). It enables the originator to be traced to its true source.
- **TCP Intercept**: Configuring TCP Intercept prevents DoS attacks by intercepting and validating the TCP connection requests.

Countermeasures

Deflect Attacks

- Systems that are set up with limited security, also known as Honeypots, act as an enticement for an attacker.
- Honeypots serve as a means for gaining information about attackers, attack techniques and tools by storing a record of the system activities.
- Use defense-in-depth approach with IPSes at different network points to divert suspicious DoS traffic to several honeypots.

Countermeasures

- **Mitigate Attacks**
  - **Load Balancing:**
    - Increase bandwidth on critical connections to absorb additional traffic generated by an attack.
    - Replicate servers to provide additional failsafe protection.
    - Balance load on each server in a multiple-server architecture to mitigates DDoS attack.

Countermeasures

- **Mitigate Attacks**
  - **Throttling:**
    - Set routers to access a server with a logic to throttle incoming traffic levels that are safe for the server.
    - Throttling helps in preventing damage to servers by controlling the DoS traffic.
    - Can be extended to throttle DDoS attack traffic and allow legitimate user traffic for better results.
  - **Drop Request**: Drop packets when a load increases.

Countermeasures

Post-Attack Forensics

- DDoS attack traffic patterns can help the network administrators to develop new filtering techniques for preventing the attack traffic from entering or leaving the networks.
- Analyze router, firewall, and IDS logs to identify the source of the DoS traffic. Try to trace back attacker IP's with the help of intermediary ISPs and law enforcement agencies.
- Traffic pattern analysis: Data can be analyzed - post-attack - to look for specific characteristics within the attacking traffic.
- Using these characteristics, the result of traffic pattern analysis can be used for updating load-balancing and throttling countermeasures.

Countermeasures

Techniques to Defend against Botnets

- **RFC 3704 Filtering**: Any traffic coming from unused or reserved IP addresses is bogus and should be filtered at the ISP before it enters the Internet link.
- **Cisco IPS Source IP Reputation Filtering**: Reputation services help in determining if an IP or service is a source of threat or not, Cisco IPS regularly updates its database with known threats such as botnets, botnet harvesters, malwares, etc. and helps in filtering DoS traffic.

Countermeasures

- **Black Hole Filtering**:
  - Black hole refers to network nodes where incoming traffic is discarded or dropped without informing the source that the data did not reach it intended recipient.
  - Black hole filtering refers to discarding packets at the routing level.
- **DDoS Prevention Offerings from ISP or DDoS Service**: Enable IP Source Guard (in CISCO) or similar features in other routers to filter traffic based on the DHCP snooping binding database or IP source bindings which prevents a bot to send spoofed packets.

Countermeasures

DoS/DDoS Countermeasures

- Use strong encryption mechanisms such as WPA2, AES 256, etc. for broadband networks to withstand against eavesdropping.
- Ensure that the software and protocols are up-to-date and scan the machines thoroughly to detect any anomalous behavior.
- Disable unused and insecure services.
- Block all inbound packets originating from the service ports to block the traffic from reflection servers.
- Update kernel to the latest release.

Countermeasures

- Prevent the transmission of the fraudulently addressed packets at ISP level.
- Implement cognitive radios in the physical layer to handle the jamming and scrambling attacks.
- Configure the firewall to deny external ICMP traffic access.
- Perform the thorough input validation.
- Prevent use of unnecessary functions such as gets, strcpy etc.
- Secure the remote administration and connectivity testing.
- Data processed by the attacker should be stopped from being executed.
- Prevent the return addresses from being overwritten.

Countermeasures

DoS/DDoS Protection at ISP Level

- Most ISPs simply blocks all the requests during a DDoS attack, denying even the legitimate traffic from accessing the service.
- ISPs offer in-the-cloud DDoS protection for Internet links so that they do not become saturated by the attack.
- Attack traffic is redirected to the ISP during the attack to be filtered and sent back.
- Administrators can request ISPs to block the original affected IP and move their site to another IP after performing DNS propagation.

Countermeasures

FortiDDoS-300A

http://www.fortinet.com

DDoS Protector

http://www.checkpoint.com

Cisco Guard XT 5650

http://www.cisco.com

Arbor Pravail: Availability Protection System

http://www.arbornetworks.com

HACKING

Is an art, practised through a creative mind.