More Denial of Service – and Defense

Information Security – Lecture 20

Aadil Zia Khan

Question

- Name some network applications that you use
  - Web browsing, clock sync, file sharing
- Which one can you use to conduct a DoS attack - describe your attack strategy
  - As long as traffic loads can be generated, any application can be used for the attacks

HTTP-Based Attacks: HTTP Flood

- Attacker bombards Web server with HTTP requests
    - Usually HTTP requests come from many different bots
- Requests can be designed to consume considerable resources
    - For example, an HTTP request to download a very large file from the target
    - Which resource will this DoS target?
        - It causes the Web server to read the file from hard disk, store it in memory, convert it into a packet stream, then transmit the packets
        - This process consumes memory, CPU processing, and bandwidth

- A variant of this attack is known as a recursive HTTP flood – also called spidering
    - Bots start from a given HTTP link and then follows all links on the provided website recursively

HTTP-Based Attacks: Slowloris

- Slowloris exploits the common server technique of using multiple threads to support multiple requests to the same server application
- It attempts to monopolize all of the available request handling threads on the Web server by sending HTTP requests that never complete
- HTTP protocol requires that a blank line must be used to indicate the end of the request headers and the beginning of the payload
  - Web server may then respond once the entire request is received

HTTP-Based Attacks: Slowloris

- Attacker establishes multiple connections to the Web server
- On each connection, he sends an incomplete request that does not include the terminating newline sequence
- The attacker sends additional header lines periodically to keep the connection alive, but never sends the terminating newline sequence
- Web server keeps the connection open, expecting more information to complete the request – eventually consuming all available Web server connections, thus rendering the Web server unavailable to respond to legitimate requests

NTP Reflection-Amplification Attacks

- Network Time Protocol (NTP) is used to synchronize system clocks
- NTP has a command called monlist, which sends the details of the last 600 hosts that have requested the time from the NTP server, back to the requester *(disabling this command protects against the attack)*
- A small request to this time server can be sent using a spoofed source IP address of some victim, which results in a response 600 times larger than the size of the request
- This becomes further amplified when using botnets that all send requests with the same spoofed IP source, which will result in a massive amount of data being sent back to the victim

Other Attacks Possible???

Any application / protocol that can generate traffic can be used for DoS attacks

- Slow Read attack
  - Attacker sends legitimate application layer requests, but reads responses very slowly, thus trying to exhaust the server's connection pool
  - This is achieved by advertising a very small number for the TCP Receive Window size, and at the same time emptying clients' TCP receive buffer slowly, which causes a very low data flow rate

Other Attacks Possible???

Any application / protocol that can generate traffic can be used for DoS attacks

- TTL expiry attack
    - When a packet is dropped due to TTL expiry, the router CPU must generate and send an ICMP time exceeded response
    - Generating many of these responses can overload the router's CPU

Other Attacks Possible???

Any application / protocol that can generate traffic can be used for DoS attacks

- ARP spoofing
    - Attacker can associate their MAC address to the IP address of another computer or gateway (like a router)
    - This causes traffic intended for the original authentic IP to be re-routed to that of the attacker, causing denial of service

Defense

What options does the system admin have to protect against the different types of DoS attacks

Defense Techniques:

- Application front-end hardware
  - It is intelligent hardware placed inside the network
  - It analyzes data packets as they enter the system, and then identifies them as priority, regular, or dangerous and doesn’t let them pass (or reach the server) if dangerous

- Firewalls
  - They can make a machine invisible outside the network
  - They can implement rules to block protocols, or drop traffic based on source or destination addresses and ports

Defense Techniques:

- Upstream filtering
  - Note that spoofing is the biggest problem
  - Every time a packet is received at the routers (or middleboxes) along the path towards the destination, they should try to determine if the source address is spoofed or not
  - Nodes inside the attacker’s ISP can do that easily
    - An ISP knows which addresses are allocated to all its customers and hence can ensure that valid source addresses are used in all packets from its customers

Defense Techniques:

- SYN Cookies
  - SYN Spoofing causes the TCP connection table to fill up
  - If that happens, the server can store the connection information inside an encrypted cookie and place it in the TCP header, instead of storing it inside the table

- Random Drop
  - If the TCP connection table fills up, the server can randomly select a connection with incomplete handshake and remove it from the table to make room for others

Defense Techniques:

- Rate Limiting & Connection Limits
  - Servers and ISPs can also place a limit on the number of connections or the amount of bandwidth a single source can have

- Slowloris Attack Prevention
  - Limit the number of connections a single IP address is allowed to make
  - Impose restrictions on the minimum transfer speed a connection is allowed to have
  - Restrict the length of time a client is allowed to stay connected

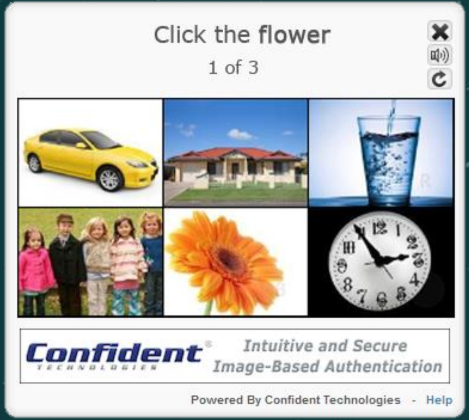
Defense Techniques:

- Smurf Attack Prevention
    - Configure individual hosts and routers to not respond to ICMP requests or broadcasts
    - Configure routers to not forward packets directed to broadcast addresses

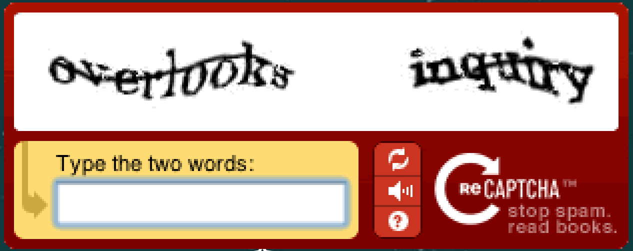
Defense Techniques:

- Blackholing and sinkholing
  - Once a victim is identified on the network, all the traffic to the attacked IP address is sent to a "black hole" (null interface or a non-existent server)

Defense Techniques:


Click the flower
1 of 3
Confident TECHNOLOGIES
Intuitive and Secure Image-Based Authentication
Powered By Confident Technologies - Help

- Captchas
  - To prevent requests from bots, the server can ask the requester to solve a captcha


overlooks
inquiry
Type the two words:
reCAPTCHA™
stop spam.
read books.