CHƯƠNG 5

1.

- Cách thức hoạt động của DDoS khuếch đại là kẻ tấn công gửi yêu cầu tra cứu tên DNS đến máy chủ DNS mở với địa chỉ nguồn được giả mạo là địa chỉ của mục tiêu. Khi máy chủ DNS gửi phản hồi bản ghi DNS, phản hồi đó sẽ được gửi đến mục tiêu. Kẻ tấn công thường sẽ gửi yêu cầu cung cấp càng nhiều thông tin vùng càng tốt để tối đa hóa hiệu ứng khuếch đại khiến thông tin phản hồi về lớn hơn yêu cầu được gửi đi gấp nhiều lần.

Source: https://www.cisa.gov/news-events/alerts/2013/03/29/dns-amplification-attacks

2.

- Khác biệt giữa bot và zombie là:

    - bot là máy tính hoạt thiết bị đã bị chiếm quyền điều khiển.

    - zombie là bot đã bị lây nhiễm phần mềm độc hại.

Srouce: https://www.universalcpareview.com/ask-joey/what-is-cybersecurity-and-what-are-the-different-types-of-cyber-attacks/

- Các công cụ phân tích lưu lượng mạng: auvik, SolarWinds NetFlow Traffic Analyzer, ManageEngine NTA

Source: https://thegioimang.vn/dien-dan/threads/10-c%C3%B4ng-c%E1%BB%A5-ph%E1%BA%A7n-m%E1%BB%81m-ph%C3%A2n-t%C3%ADch-l%C6%B0u-l%C6%B0%E1%BB%A3ng-m%E1%BA%A1ng-nta-network-traffic-analyzer-t%E1%BB%91t-nh%E1%BA%A5t.30312/

3.

- Capcha là 1 giải pháp chống DoS/DDoS cho trang web chi phí thấp nhất (dưới 1 usd cho 1000 lượt giải)

Source: https://www.hcaptcha.com/report-how-much-is-a-recaptcha-really-worth

4.

- Tin tặc sử dụng hping3 để tìm hiểu về HDH, cổng mở, các dịch vụ đang chạy, các ứng dụng đã cài đặt và đang chạy

source: https://www.okta.com/identity-101/hping/

- Cách phòng thủ đơn giản nhất khi bị tấn công hping3 là lọc và chặn các gói tin đó.

Source: https://www.redlegg.com/blog/3-tools-to-test-denial-of-service-vulnerability

5.

- Khác nhau giữa SYN FLOOD (SF) và SYN SPOOFING (SS) là SF dùng chính ip của attacker, còn SS dùng IP giả mạo.

source: https://www.indusface.com/blog/what-is-syn-synchronize-attack-how-the-attack-works-and-how-to-prevent-the-syn-attack/

- Website gần như không bị tấn công DoS/DdoS là dạng website tĩnh,

6.

- Máy chủ cung cấp dịch vụ thời gian thực như VoIP dễ bị tấn công UDP Floodting. Vì giao thức UDP có có tốc độ cao đáp ứng thời gian thực nhưng không an toàn. UDP không có kết nối như TCP nên các gói tin có thể được gửi tràn lan đến máy chủ.

source: https://www.onsip.com/voip-resources/voip-fundamentals/udp-versus-tcp-for-voip

7.

- Trên Linux có thể sử dụng ứng dụng "iptables" để chặn ICMP Flood

- câu lệnh: # iptables -A INPUT -p icmp --icmp-type echo-request -j REJECT

Srouce: https://kdata.vn/tin-tuc/huong-dan-cach-chan-ping-chan-giao-thuc-icmp-tren-linux

8.

- Attack Map còn được gọi là bản đồ đe dọa mạng, là biểu diễn trực quan về các cuộc tấn công mạng theo thời gian thực hoặc lịch sử trên mạng, thiết bị và hệ thống máy tính. Chúng được thiết kế để phát hiện và ứng phó với các mối đe dọa mạng , sử dụng các nguồn dữ liệu và kỹ thuật trực quan hóa để xác định các mẫu và lỗ hổng tiềm ẩn.

Srouce: https://www.splunk.com/en_us/blog/learn/cyberattack-maps.html

- Trang web thể hiện attack map: https://cybermap.kaspersky.com/

- Mô tả một số ký hiệu:

- OAS (On-Access Scan): hiển thị luồng phát hiện phần mềm độc hại trong quá trình Quét khi truy cập, tức là khi các đối tượng được truy cập trong các hoạt động mở, sao chép, chạy hoặc lưu.

- ODS (On-Demand Scan): hiển thị luồng phát hiện phần mềm độc hại trong quá trình Quét theo yêu cầu khi người dùng chọn thủ công tùy chọn 'Quét vi-rút' trong menu ngữ cảnh.

- MAV (Mail-Anti-Virus): hiển thị luồng phát hiện phần mềm độc hại trong quá trình quét Mail Anti-Virus khi các đối tượng mới xuất hiện trong ứng dụng email (Outlook, The Bat, Thunderbird). MAV quét các tin nhắn đến và gọi OAS khi lưu tệp đính kèm vào đĩa.

9.

- Cập nhật HDH không hạn chế được những hậu quả của tấn công DoS.

- Cách phòng thủ tạm thời, ngay lập tức khi bị tấn công DoS:

- Liên hệ với bên cung cấp hosting ngay sau khi phát hiện bị tấn công.

- Thực hiện kế hoạch dự phòng.

10.

- Ngoài DoS ra thì bot còn có thể thực hiện hành động như đánh cắp dữ liệu, phát tán nội dung spam, bot tự động hóa thao tác đăng nhập sau khi đánh cắp được list user-password,...