

**ĐẠI HỌC ĐÀ NẴNG**

**TRƯỜNG ĐẠI HỌC BÁCH KHOA**

**KHOA CÔNG NGHỆ THÔNG TIN**

Tel. (+84.0236) 3736949, Fax. (+84.0236) 3842771

Website: itf.dut.udn.vn, E-mail: cntt@dut.udn.vn



**BÁO CÁO**

**ĐỒ ÁN CHUYÊN NGÀNH MẠNG**

**NGÀNH CÔNG NGHỆ THÔNG TIN**

**Tìm hiểu về DoS và cách phòng chống**

**SINH VIÊN : Võ Văn Tâm**

**MÃ SINH VIÊN : 102170053**

**LỚP : 17T1**

**CBHD : Nguyễn Thị Lệ Quyên**

**Đà Nẵng, 07/2021**

1. **Lịch sử tấn công DDoS**
2. Mục tiêu
3. Các cuộc tấn công
4. **Định nghĩa về tấn công DoS**
5. Mục tiêu của tấn công DoS
6. Mục tiêu của kẻ tấn công thường sử dụng tấn công DoS
7. **Các dạng tấn công**
8. Nhận dạng kiểu tấn công DDoS
9. Các đặc tính của tấn công DDoS
10. Các phương pháp tấn công
    1. Tấn công Smurf
    2. Tấn công Buffer Overflow
    3. Tấn công Ping of Death
    4. Tấn công teardrop
    5. Tấn công SYN
11. **Mạng BOT NET**
12. Ý nghĩa của mạng BOT
13. Mạng BOT
14. Mạng Botnet
15. Mục đích sử dụng mạng Botnets
16. Các dạng của mạng BOT
17. Các bước xây dựng mạng Botnet
18. **Phòng chống DDoS**
19. Phòng chống DDoS
20. Kết luận

**VI. Demo tấn công và phòng thủ DOS**

1. Tấn công bằng Slowloris
2. Cấu hình ufw trên Web server
3. **Lịch sử tấn công DDOS**
4. **Mục tiêu**

* Mục tiêu của các cuộc tấn công thường là vào các trang web lớn và các tổ chức thương mại điện tử trên Internet trở nên quá tải. Người dùng gặp khó khăn, hay thậm chí không thể truy nhập vào các trang web, dịch vụ này.

1. **Các cuộc tấn công** 
   * Ngày 7/3/2000, yahoo.com đã phải ngưng phục vụ hàng tram triệu user trên toàn thế giới trong nhiều giờ liên. Vài giờ sau, Yahoo đã tìm ra nguyên nhân gây nên tình trạng này, họ đang phải gánh chịu một đợt tấn công DDoS với quy mô vài ngàn máy tính liên tục gửi hàng triệu request đến các server dịch vụ làm các server này không thể phục vụ các user thông thường khác.
   * Vài ngày sau, một sự kiện tương tự diễn ra nhưng có phần “ồn ào” hơn là một trong các nạn nhân mới là hang tin CNN, amazon.com, buy.com, Zdnet.com E-trade.com, Ebay.com. Tất cả các nạn nhân là những gã khổng lồ trên Internet thuộc nhiều lĩnh vực khác nhau. Theo Yankke Group, tổng thiệt hại do cuộc tấn công lên đến 1,2 triệu USD, nhưng nhưng không đáng kể bằng sự mất mát về lòng tin của khách hàng, uy tín của các công ti là không thể tính được.
   * Làm đảo lộn mọi dứ tính, thủ phạm là một cậu bé 15 tuổi người Canada, với nick name là “mafiaboy”. Lại một kẻ thiên tài bẩm sinh như Kenvin Mitnick xuất hiện? Không. Mafiaboy chỉ tìm tòi và download về một số công cụ của các hacker. Cậu dung một công cụ DDoS có tên là TrinOO để gây rac các cuộc tấn công kiểu DDoS khủng khiếp trên.
   * Vào 15/8/2003, Microsoft đã chịu đợt tấn công DDoS cực mạnh và làm gián đoạn website trong vòng 2 giờ.
   * Vào lúc 15:09 giờ GMT ngày 27/3/2003 toàn bộ phiên bản tiếng anh của website AI-Jazeera bị tấn công làm gián đoạn trong nhiều giờ.
2. **Định nghĩa về tấn công DoS**

* Tấn công DoS là kiểu tấn công vô cùng nguy hiểm, để hiểu được cần phải nắm rõ định nghĩa của tấn công DoS và các dạng tấn công DoS.
* Tấn công DoS là một kiểu tấn công mà một người làm cho một hệ thống không thể sử dụng, hoặc làm cho hệ thống đó chậm đi một cách đáng kể với người dùng bình thường, bằng cách làm quá tải tài nguyên hệ thống.
* Nếu kẻ tấn công không có khả năng thâm nhập được vào hệ thống, thì chúng cố gắng tìm cách làm cho hệ thống đó sụp đổ và không có khả năng phục vụ người dùng bình thường là tấn công Denial of Service (DoS).

Mặc dù tấn công không có khả năng thâm nhập vào dữ liệu thực của hệ thống nhưng nó có thể làm gián đoạn cách dịch vụ mà hệ thống đó cung cấp. Như định nghĩa trên DoS khi tấn công vào một hệ thống sẽ khai thác những cái yếu nhất của hệ thống để tấn công, những mục đích của tấn công DoS

1. **Các mục đích của tấn công DoS**

* Cố gắng chiếm băng thông mạng và làm hệ thống mạng bị ngập (flood), khi đó hệ thống mạng sẽ không có khả năng đáp ứng những yêu cầu dịch vụ khác cho người dùng bình thường.
* Cố gắng ngắt kết nối giữa hai máy, và ngăn chặn quá trình truy cập vào dịch vụ.
* Cố gắng ngăn chặn những người dùng cụ thể vào một dịch vụ nào đó.
* Cố gắng ngăn chặn các dịch vụ không có người khác có khả năng truy cập vào.
* Khi tấn công DoS xảy ra người dùng có cảm giác khi truy cập vào dịch vụ đó bị:
  + Disable Network – Tắt mạng
  + Disable Organization – Tổ chức không hoạt động
  + Financial Loss – Tài chính bị mất

1. **Mục tiêu mà kẻ tấn công thường sử dụng tấn công DoS**

Tấn công DoS xảy ra khi kẻ tấn công sử dụng hết tài nguyên của hệ thống và hệ thống không thể đáp ứng cho người dùng bình thường được vậy các tài nguyên chúng thường sử dụng tấn công là gì:

* Tạo ra sự khan hiếm, những giới hạn và không đổi mới tài nguyên.
* Băng thông của hệ thống mạng (Network Bandwidth), bộ nhớ, và CPU Time hay cấu trúc dữ liệu đều là mục tiêu của tấn công DoS.
* Tấn công vào hệ thống khác phục vụ cho máy tính như: Hệ thống điều hòa, hệ thống điện, hệ thống làm mát và nhiều tài nguyên khác của doanh nghiệp.
* Phá hủy hay đổi thông tin cấu hình.
* Phá hủy tầng vật lý hoặc các thiết bị mạng như nguồn điện, điều hòa,…

1. **Các dạng tấn công**

**Tấn công Denial of Service chia ra làm hai loại tấn công:**

* Tấn công DoS: Tấn công từ một cá thể, hay tập hợp các cá thể.
* Tấn công DDoS: Đây là sự tấn công từ một mạng máy tính được thiết kế để tấn công tới một mục đích cụ thể nào đó.

1. **Nhận dạng DDoS**

Đây là chìa khóa quan trọng cho việc hình thành biện pháp khắc phục tình trạng trì trệ do DDoS tạo ra và tạo điều kiện cho người dùng thực sự có hội sử dụng dịch vụ. Mỗi dạng DDoS có dấu hiệu và đặc tính khác nhau cho nên việc nhận diện DDoS là điều kiện quan trọng đứng sau việc gia tăng băng thông và tài nguyên. Băng thông và tài nguyên luôn luôn có giới hạn nhất định cho nên việc nhận dạng DDoS giúp cản lọc và tách rời chúng một cách hữu hiệu.

1. **Các đặc tính của tấn công DDoS**

* Nó được tấn công từ một hệ thống các máy tính cực lớn trên Internet, và thường dựa vào các dịch vụ có sẵn trên các máy tính trong mạng Botnet.
* Các dịch vụ tấn công được điều khiển từ những “Primary Victim” trong khi các máy tính bị chiếm quyền sử dụng trong mạng Bot được sử dụng để tấn công thường được gọi là “secondary victims”.
* Là dạng tấn công rất khó có thể phát hiện tấn công này được sinh ra từ nhiều địa chỉ IP khác nhau trên Internet.
* Nếu một địa chỉ IP tấn công một công ty, nó có thể được chặn bởi Firewall. Nếu nó từ 30.000 địa chỉ IP khác, thì điều này là vô cùng khó khăn.

1. **Các phương pháp tấn công**

Tấn công từ chối dịch vụ có thể được thực hiện theo một số các nhất định. Có năm kiểu tấn công cơ bản sau:

* Nhằm tiêu tốn tài nguyên tính toàn như băng thông, dung lượng đĩa cứng hoặc thời gian xử lý.
* Phá vỡ các thông tin cấu hình như thông tin định tuyến.
* Phá vỡ các trạng thái thông tin như việc tự động reset lại các phiên TCP.
* Phá vỡ các thành phần vật lý của mạng máy tính.
* Làm tắc nghẽn thông tin liên lạc có chủ đích giữa người dùng và nạn nhân đến việc liên lạc giữa hai bên không được thông suốt.

Một việc tấn công từ chối dịch vụ có thể bao gồm thực thi Malware nhằm:

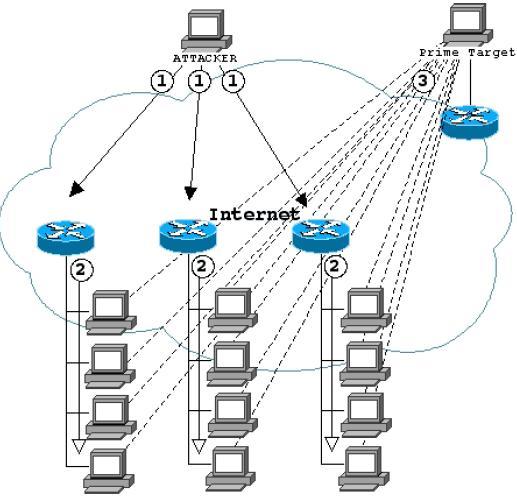
* Làm quá tải năng lực xử lý, dẫn đến hệ thống không thể thực thi bất kì một công việc nào khác.
* Những lỗi tức thì trong Microcode của máy tính.
* Những lỗi gọi thức thì trong chuỗi chỉ thị, dẫn đến máy tính rời vào trạng thái hoạt động không ổn định hoặc bị đơ.
* Những lỗi có thể khai thác được ở hệ điều hành dẫn đến việc thiếu thốn tài nguyên.
* Gây Crash hệ thống.
* Tấn công từ chối dịch vụ iFrame: trong một trang HTML có thể gọi đến một trang web nào đó với rất nhiều yêu cầu và trong rất nhiều lần cho đến khi băng thông của trang web bị quá tải.

**3.1 Tấn công Smurf**

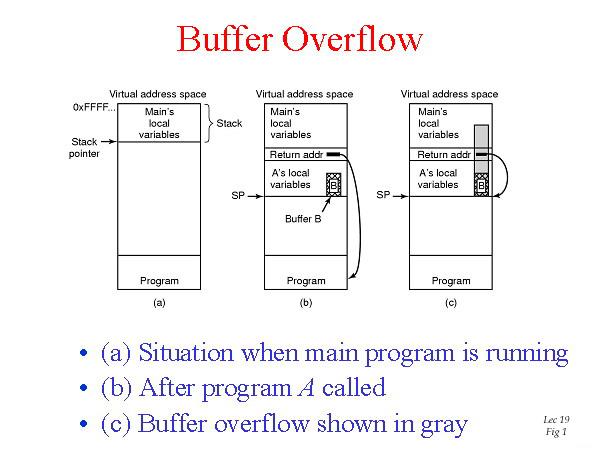
* Là thủ phạm sinh nhiều giao tiếp ICMP (ping) tới các địa chỉ Broadcast của nhiều mạng với địa chỉ nguồn là mục tiêu cần tấn công.

Khi ping đến một địa chỉ là quá trình hai chiều – Khi máy A ping tới máy B máy B reply lại hoàn tất quá trình. Khi ping tới địa chỉ Broadcast của mạng nào đó thì toàn bộ các máy tính trong mạng đó sẽ Reply lại. Thay đổi địa chỉ nguồn là máy C và ping tới địa chỉ Broadcast của của một mạng nào đó, thì toàn bộ các máy tính trong mạng đó sẽ Reply lại vào máy C đó là tấn công Smurf.

* Kết quả đích tấn công sẽ phải chịu nhận một đợt Reply gói ICMP cực lớn và làm cho mạng bị rớt hoặc bị chậm lại không có khả năng đáp ứng các dịch vụ khác.
* Quá trình này được khuếch đại khi có luông ping reply từ một mạng được kết nối với nhau (mạng BOT).
* Tấn công Fraggle, chúng sử dụng UDP echo và tương tự như tấn công Smurf.

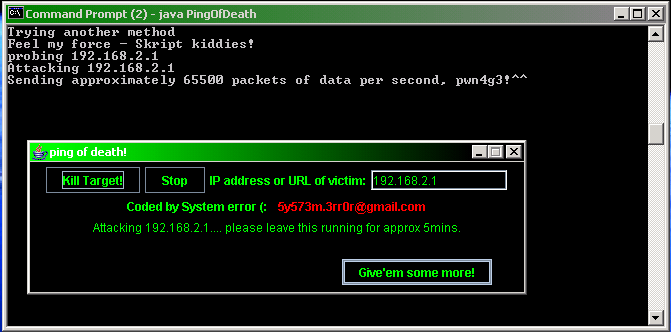


**3.2 Tấn công Buffer overflow**

* Buffer Overflow xảy ra tại bất kỳ điểm nào có chương trình ghi lượng thông tin lớn hơn dụng lượng của bộ nhớ đệm trong bộ nhớ.
* Kẻ tấn công có thể ghi đè lên dữ liệu và điều khiển các chương trình và đánh cắp quyền điều khiển của một số chương trình nhằm thực thi các đoạn mã nguy hiểm.
* Các lỗi tràn bộ đệm có thể làm cho tiến trình bị đổ vỡ hoặc cho kết quả sai. Các lỗi này có thể được kích hoạt bởi các dữ liệu vào được thiết đặc biệt để thực thi các đoạn mã phá hoại hoặc để làm cho chương trình hoạt động không như mong đợi. Bằng cách đó các lỗi tràn bộ đệm gây ra nhiều lỗ hổng bảo mật đối với phần mềm và tạo cơ sở cho nhiều thủ thuật khai thác.

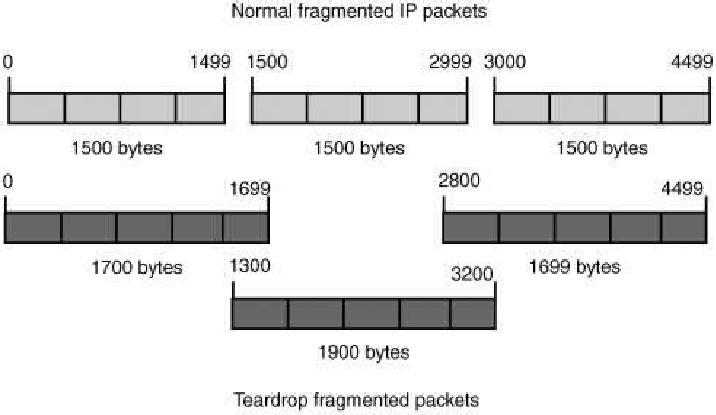
**3.3 Tấn công Ping of Death**

* Kẻ tấn công gửi những gói tin IP lớn hơn số lượng bytes cho phép của IP là 65.536 bytes
* Quá trình chia nhỏ gói tin IP thành những phần nhỏ được thực hiện bởi layer II.
* Quá trình chia nhỏ có thể thực hiện với gói IP lớn hơn 65.536 bytes. Nhưng hệ điều hành không thể nhận biết được độ lớn của gói tin này và sẽ bị khởi động lại, hay đơn giản là sẽ bị gián đoạn giao tiếp.

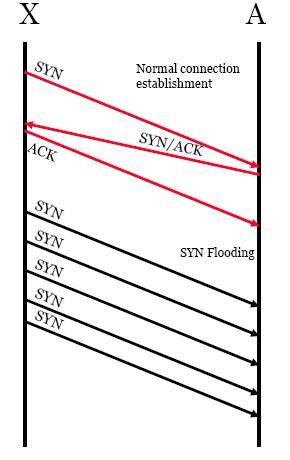


**3.4 Tấn công Teardrop**

* Gói tin IP rất lớn khi đến các Router sẽ bị chia nhỏ thành nhiều phần nhỏ.
* Kẻ tấn công sử dụng gói IP với các thông số khó hiểu để chia ra các phần nhỏ (fragment).
* Nếu hệ điều hành nhận được các gói tin đã được chia nhỏ và không thể hiểu được, hệ thống cố gắng build lại gói tin và điều đó chiếm một phần tài nguyên hệ thống, nếu quá trình đó xảy ra liên tục thống không còn tài nguyên cho các ứng dụng khác, phục vụ server khác.
* Dựa vào quá trình di chuyển dữ liệu từ máy tính nguồn tới máy tính đích. Các mảnh nhỏ đến hệ thống đích sẽ dựa vào giá trị offset để sắp xếp các mảnh lại với nhau theo đúng thứ tự như ban đầu. Tận dung điều đó Hacker gửi đến hệ điều thống một loạt gói tin packets với giá trị offset chồng chéo lên nhau. Hệ thống sẽ không thể nào sắp xếp lại các packets này, vì vậy hệ thống đích có thể bị treo, reboot hoặc ngừng hoạt động nếu số lượng packets với giá trị offset chồng chéo lên nhau quá lớn. Các hệ điều hành như Windows NT, Windows 95… thậm chí cả Linux trước khi lên phiên bản 2.1.63 là rất dễ bị tấn công bởi phương pháp này.





* 1. **Tấn công SYN**
* Kẻ tấn công gửi các yêu cầu (Request ảo) TCP SYN tới máy chủ bị tấn công. Để xử lý lượng gói tin SYN này hệ thống cần tốn một lượng bộ nhớ cho kết nối.
* Khi có rất nhiều gói SYN ảo tới máy chủ và chiếm hết các yêu cầu xử lý của máy chủ. Một người dùng bình thường kết nối tới máy chủ ban đầu thực hiện Request TCP SYN và lúc này máy chủ không còn khả năng đáp lại – kết nối không được thực hiện.
* Đây là kiểu tấn công mà kẻ tấn công lợi dụng quá trình giao tiếp của TCP theo Three-way.
* Các đoạn mã nguy hiểm có khả năng sinh ra một lượng cực lớn các gói tin TCP SYN tới máy chủ bị tấn công, địa chỉ IP nguồn của gói tin đã bị thay đổi và đó chính là tấn công DoS.
* Hình bên thể hiện các giao tiếp bình thường tới máy chủ và bên dưới thể hiện khi máy chủ bị tấn công gói SYN đến sé rất nhiều trong khi đó khả năng trả lời của máy chủ lại có hạn và khi đó máy chủ sẽ từ chối các truy cập hợp pháp.
* Quá trình TCP Three-way handshake được thực hiện: Khi máy A muốn giao tiếp với máy B. (1) máy A bắn ra một gói TCP SYN tới máy B – (2) máy B khi nhận được gói SYN từ A sẽ gửi lại máy A gói ACK đồng ý kết nối – (3) máy A gửi lại máy B goi ACK và bắt đầu các giao tiếp dữ liệu.
* Máy A và máy B sẽ dữ kết nối ít nhất 75 giây, sau đó lại thực hiện một quá trình TCP Three-way handshake lần nữa để thực hiện phiên kết nối tiếp theo để trao đổi dữ liệu.
* Kẻ tấn công đã lợi dụng kẽ hở này để thực hiện hành vi tấn công nhằm sử dụng hết tài nguyên của hệ thống bằng cách giảm thời gian yêu cầu Three-way handshake xuống nhất nhỏ và không gửi lại gói ACK, cứ bắn gói SYN ra liên tục trong một thời gian nhất định và không bao giờ trả lại gói SYN & ACK từ máy tấn công.
* Với nguyên tắc chỉ chấp nhận gói SYN từ một máy tới hệ thống sau mỗi 75 giây nếu địa chỉ nào vi phạm sẽ chuyển vào Rule deny access sẽ ngăn cản tấn công này.

1. **Mạng BOT NET**
   1. **Ý nghĩa mạng BOT NET**

* Khi sử dụng một Tool tấn công DDoS tới một máy chủ đôi khi không gây ảnh hưởng gì tới máy chủ - Giả sử bạn sử dụng Tool Ping of Death tới một máy chủ, trong đó máy chủ kết nối với mạng tốc độ 100bps bạn kết nối tới máy chủ tốc độ 3bps – vậy tấn công của bạn không có ý nghĩa gì.
* Nhưng hãy tưởng tượng có 1000 người như bạn cùng một lúc tấn công vào máy chủ kia khi đó toàn bộ băng thông của 1000 người công lại tối đã đạt 3Gbps và tốc độ kết nối của máy chủ là 100Mbps vậy kết quả sẽ ra sao các bạn có khả năng tưởng tượng.
* Nhưng làm cách nào để có 1000 máy tính kết nối với mạng – đi mua 1000 chiếc máy tính và 1000 thuê bao kết nối – chắc chắn không ai làm như vậy và cũng không kẻ tấn công nào lại sử dụng phương pháp này cả.
* Kẻ tấn công xây dựng một mạng hàng nghìn máy tính kết nối Internet (Có mạng BOT lên tới 400.000 máy). Vậy làm thế nào hacker có khả năng lợi dụng người kết nối tới Internet để xây dựng mạng BOT.
* Khi có trong tay mạng BOT kẻ tấn công sử dụng những tool tấn công đơn giản để tấn công vào một hệ thống máy tính. Dựa vào những truy cập hoàn toàn hợp lệ của hệ thống, cùng một lúc Hacker sử dụng một dịch vụ của máy chủ, hãy thử tưởng tượng khi kẻ tấn công có trong tay 400.000 máy tính cùng một lúc ra lệnh cho chúng download một file trên trang web của bạn. Và đó chính là tấn công DDoS – Distributed Denial of Service.
  1. **Mạng BOT**
* BOT từ viết tắt của từ RoBOT
* IRCbot – còn được gọi là zombie hay drone.
* Internet Relay Chat (IRC) là một dạng truyền dữ liệu thời gian thực trên Internet. Nó thường được thiết kế sao cho một người có thể nhắn được cho một Group và mỗi người có thể giao tiếp với nhau với một kênh khác nhau được gọi là – Channels.
* Đầu tiên BOT kết nối kênh IRC với IRC server và đời giao tiếp giữa những người với nhau.
* Kẻ tấn công có thể điều khiển mạng BOT và sử dụng mạng BOT cũng như sử dụng nằm một mục đích nào đó.
* Nhiều mạng BOT kết nối với nhau người ta gọi là BOTNET – botnet.

**3. Mạng Botnet**

* Mạng Botnet bao gồm nhiều máy tính.
* Nó được sử dụng cho mục đích tấn công DDoS.
* Một mạng Botnet nhỏ có thể chỉ bao gồm 1000 máy tính hãy tưởng tượng mỗi máy tính kết nối tới Internet tốc độ chỉ 128Kbps thì mạng Botnet này có khả năng tao bang thông là 1000x128 ~ 100Mbps – Đây là một con số thể hiện bảng thông mà khó một Hosting nào có thể share cho mỗi trang web của mình.

1. **Mục đích sử dụng mạng Botnets.**

* Tấn công Distributed of Service – DdoS: Botnet được sử dụng cho tấn công DDoS.
* Spamming: Mở một SOCK v4/v5 Proxy server cho Spamming.
* Sniffing traffic: Bot cũng có thể sử dụng các gói tin có sniffer (tóm được các giao tiếp mạng) sau khi tóm được các gói tin nó cố gắng giải mã gói tin để lấy được các nội dung có ý nghĩa như tài khoản ngân hàng và nhiều thông tin có giá trị khác của người sử dụng.
* Keylogging: Với sự trợ giúp của keylogger rất nhiều thông tin nhạy cảm của người dùng có thể bị kẻ tấn công khai thác như tài khoản trên e-bank, cũng như nhiều tài khoản khác.
* Cài đặt và lây nhiễm chương trình độc hại: Botnet có thể sử dụng để tạo ra mạng những BOT mới.
* Cài đặt những quảng cáo Popup: Tự động bật ra những quảng cáo không mong muốn với người dùng.
* Google Adsense abuse: Tự động thay đổi kết quả tìm kiếm hiện thị mỗi khi sử dụng dịch vụ tìm kiếm của Google, khi thay đổi kết quả nó sẽ lừa người dùng kích vào những trang web nguy hiểm.

1. **Các dạng mạng BOT.**

Agobot/Phabot/Forbot/XtremBot

* Đây là những bot được viết bằng C++ trên nền tảng Cross-platform và mã nguồn được tìm trên GPL. Agobot được viết bởi Ago nick name được người ta biết đến là Wonk, một thanh niên trẻ người Đức – đã bị bắt hồi tháng 5 năm 2004 với tội danh tội phạm máy tính.
* Agobot có khả năng sử dụng NTFS Alternate Data Stream (ADS) và một loại Rootkit nằm ẩn các tiến trình đang chạy trên hệ thống

SDBot/Rbot/Urbot/UrXbot

* SDBot được viết bằng ngôn ngữ C và cũng được public bởi GPL. Nó được coi là tiền thân của Rbot, Rxbot, UrBot, UrXbot, JrBot.

mIRC-Based Bots – GT-Bots

* GT được viết từ hai từ Global Threat và tên thường được sử dụng cho tất cả các mIRC-scripted bots. Nó có khả năng sử dụng phần mềm IM và mIRC để thiết lập một số script và một đoạn mã khác

1. **Các bước xây dựng mạng BOT NET**

**Bước 1: Các lây nhiễm vào máy tính.**

* Điều đầu tiên kẻ tấn công lừa cho người dùng chạy file “chess.exe”, một Agobot thường copy chúng vào hệ thống và sẽ thêm các thông số trong registry để đảm bảo sẽ chạy cùng với hệ thống khi khởi động. Trong Registry có các vị trí cho các ứng dụng chạy lúc khởi động lại.

*HKLM\Software\Microsoft\Windows\CurrentVersion\Run*

*HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices*

**Bước 2: Cách lây lan và xây dựng tạo mạng BOTNET**

* Sau khi trong hệ thống mạng có một máy tính bị nhiễm Agobot, nó sẽ tự động tìm kiếm các máy tính khác trong hệ thống và lây nhiễm sử dụng các lỗ hổng trong tài nguyên được chia sẻ trong hệ thống mạng.
* Chúng thường cố gắng kết nối tới các dữ liệu share mặc định dành cho các ứng dụng quản trị (administrator or administrative) ví dụ như: C$, D$, E$ và print$ bằng cách đoán usernames và password để có thể truy cập được vào một hệ thống khác và lây nhiễm.
* Agobot có thể lây lan rất nhanh bởi chúng có khả năng tận dụng các điểm yếu trong hệ điều hành Windows, hay các ứng dụng, các dịch vụ chạy trên hệ thống.

**Bước 3: Kết nối vào IRC.**

* Bước tiếp theo của Agobot sẽ tạo ra một IRC-Controlled Backdoor để mở các yếu tố cần thiết, và kết nối tới mạng Botnet thông qua IRC-Control, sau khi kết nối nó sẽ mở những dịch vụ cần thiết để khi có yêu cầu chúng sẽ được điều khiển bởi kẻ tấn công thông qua kênh giao tiếp IRC.

**Bước 4: Điều khiển tấn công từ mạng BotNet**.

* Kẻ tấn công điều khiển các máy trong mạng Agobot download những file .exe về chạy trên máy.
* Lấy toàn bộ thông tin liên quan và cần thiết trên hệ thống mà kẻ tấn công muốn.
* Chạy những file khác trên hệ thống đáp ứng yêu cầu của kẻ tấn công.
* Chạy những chương trình DDoS tấn công hệ thống khác.

1. **Phòng chống DDoS**
   1. **Phòng chống DDoS**

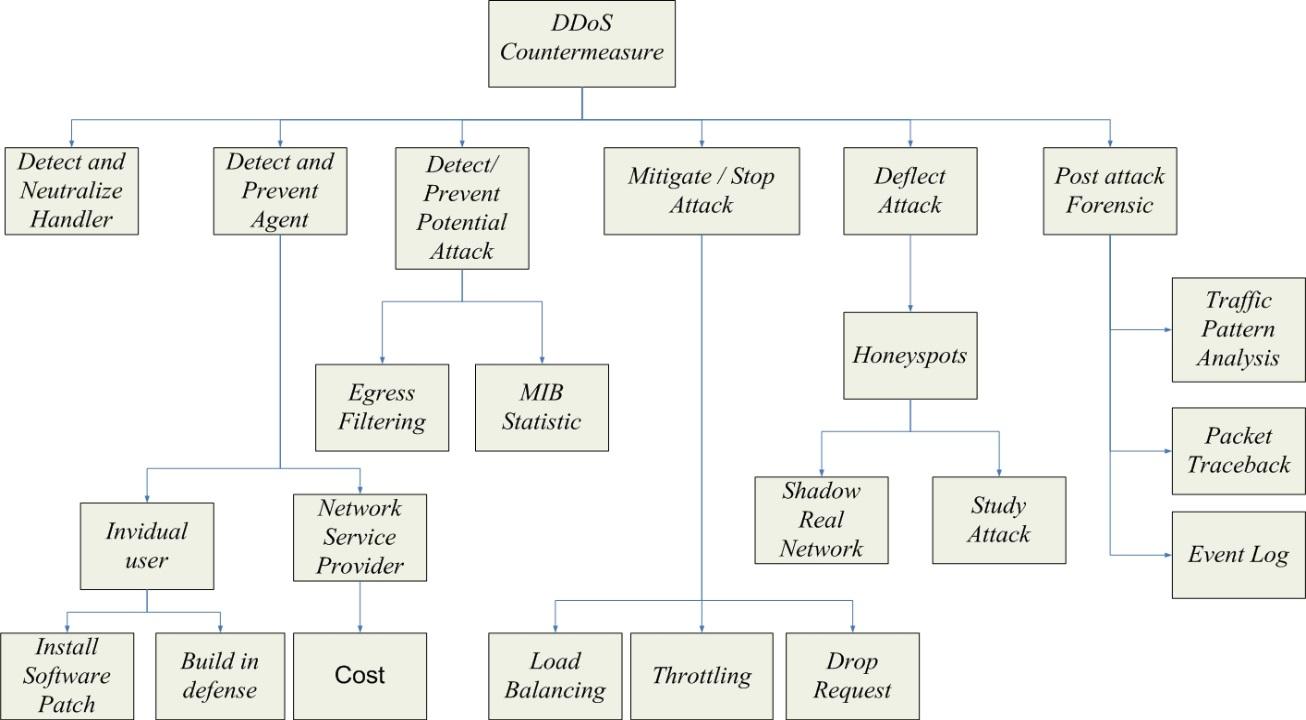
Có rất nhiều giải pháp và ý tưởng được đưa ra nhằm đối phó với các cuộc tấn công kiểu DDoS. Tuy nhiên không có giải pháp và ý tưởng nào là giải quyết trọn vẹn bài toán Phòng chống DDoS. Các hình thái khác nhau của DDoS liên tục xuất hiện theo thời gian song song với các giải pháp đối phó, tuy nhiên cuộc đua vẫn tuân theo quy luật tất yếu của bảo mật máy tính: “Hacker luôn đi trước giới bảo mật một bước”.

**Có ba giai đoạn chính trong quá trình Phòng chống DDoS:**

- Giai đoạn ngăn ngừa: tối thiểu hóa lượng Agent, tìm và vô hiệu hóa các Handler.

- Giai đoạn đối đầu với cuộc tấn công: Phát hiện và ngăn chặn cuộc tấn công, làm suy giảm và dừng cuộc tấn công, chuyển hướng cuộc tấn công.

- Giai đoạn sau khi cuộc tấn công xảy ra: thu thập chứng cứ và rút kinh nghiệm.





* 1. **Tối thiểu hóa lượng Agent**

**Từ phía người dùng**: một phương pháp rất tốt để ngăn ngừa tấn công DDoS là từng người dùng Internet sẽ tự đề phòng không để bị lợi dụng tấn công hệ thống khác. Muốn đạt được điều này thì ý thức và kỹ thuật phòng chống phải được phổ biến rộng rãi cho mọi người dùng. Mạng lưới Botnet sẽ không bao giờ hình thành nếu không có người nào bị lợi dụng trở thành Agent. Mọi người dùng phải liên tục thực hiện các quá trình bảo mật trên máy vi tính của mình. Họ phải tự kiểm tra sự hiện diện của Agent trên máy của mình, điều này là rất khó khăn đối với những người dùng thông thường. Một giải pháp đơn giản là nên cài đặt và update liên tục các software như antivirus, antitrojan và các bản patch của hệ điều hành.

**Từ phía Network Service Provider**: Thay đổi cách tính tiền dịch vụ truy cập theo dung lượng sẽ làm cho user lưu ý đến những gì họ gửi, như vậy về mặt ý thức tăng cường phát hiện DDoS Agent sẽ tự nâng cao ở mỗi người dùng.

#### **Tìm và vô hiệu hóa các Handler**

Một nhân tố vô cùng quan trọng trong mạng Botnet là Handler, nếu có thể phát hiện và vô hiệu hóa Handler thì khả năng Phòng chống DDoS thành công là rất cao. Bằng cách theo dõi các giao tiếp giữa Handler và Client hay Handler và Agent ta có thể phát hiện ra vị trí của Handler. Do một Handler quản lý nhiều, nên triệt tiêu được một Handler cũng có nghĩa là loại bỏ một lượng đáng kể các Agent trong mạng Botnet.

* 1. **Phát hiện dấu hiệu của cuộc tấn công**

**Có nhiều kỹ thuật được áp dụng:**

* **Egress Filtering**: Kỹ thuật này kiểm tra xem một packet có đủ tiêu chuẩn ra khỏi một subnet hay không dựa trên cơ sở gateway của mộtsubnet luôn biết được địa chỉ IP của các máy thuộc subnet. Các packet từ bên trong subnet gửi ra ngoài với địa chỉ nguồn không hợp lệ sẽ bị giữ lại để điều tra nguyên nhân. Nếu kỹ thuật này được áp dụng trên tất cả các subnet của Internet thì khái nhiệm giả mạo địa chỉ IP sẽ không còn tồn tại.
* **MIB statistics**: trong Management Information Base (SNMP-Simple Network Management Protocol ) của router luôn có thông tin thống kê về sự biến thiên trạng thái của mạng. Nếu ta giám sát chặt chẽ các thống kê của Protocol ICMP, UDP và TCP ta sẽ có khả năng phát hiện được thời điểm bắt đầu của cuộc tấn công để tạo “quỹ thời gian vàng” cho việc xử lý tình huống.

**1.4 làm suy giảm hoặc ngừng cuộc tấn công**

Dùng các kỹ thuật sau:

* **Load balancing**: Thiết lập kiến trúc cân bằng tải cho các server trọng điểm sẽ làm gia tăng thời gian chống chọi của hệ thống với cuộc tấn công DDoS. Tuy nhiên, điều này không có ý nghĩa lắm về mặt thực tiễn vì quy mô của cuộc tấn công là không có giới hạn.
* **Throttling**: Thiết lập cơ chế điều tiết trên router, quy định một khoảng tải hợp lý mà server bên trong có thể xử lý được. Phương pháp này cũng có thể được dùng để ngăn chặn khả năng DDoS traffic không cho user truy cập dịch vụ. Hạn chế của kỹ thuật này là không phân biệt được giữa các loại traffic, đôi khi làm dịch vụ bị gián đoạn với user, DDoS traffic vẫn có thể xâm nhập vào mạng dịch vụ nhưng với số lượng hữu hạn.
* **Drop request**: Thiết lập cơ chế drop request nếu nó vi phạm một số quy định như: thời gian delay kéo dài, tốn nhiều tài nguyên để xử lý, gây deadlock. Kỹ thuật này triệt tiêu khả năng làm cạn kiệt năng lực hệ thống, tuy nhiên nó cũng giới hạn một số hoạt động thông thường của hệ thống, cần cân nhắc khi sử dụng.

**1.5 Chuyển hướng cuộc tấn công**

**Honeyspots**: Một kỹ thuật đang được nghiên cứu là Honeyspots. Honeyspots là một hệ thống được thiết kế nhằm đánh lừa attacker tấn công vào khi xâm nhập hệ thống mà không chú ý đến hệ thống quan trọng thực sự.

Honeyspots không chỉ đóng vai trò “Lê Lai cứu chúa” mà còn rất hiệu quả trong việc phát hiện và xử lý xâm nhập, vì trên Honeyspots đã thiết lập sẵn các cơ chế giám sát và báo động.

Ngoài ra, Honeyspots còn có giá trị trong việc học hỏi và rút kinh nghiệm từ Attacker, do Honeyspots ghi nhận khá chi tiết mọi động thái của attacker trên hệ thống. Nếu attacker bị đánh lừa và cài đặt Agent hay Handler lên Honeyspots thì khả năng bị triệt tiêu toàn bộ mạng Botnet là rất cao.

* 1. **Giai đoạn sau tấn công**

Trong giai đoạn này thông thường thực hiện các công việc sau:

* + **Traffic Pattern Analysis:** Nếu dữ liệu về thống kê biến thiên lượng traffic theo thời gian đã được lưu lại thì sẽ được đưa ra phân tích. Quá trình phân tích này rất có ích cho việc tinh chỉnh lại các hệ thống Load Balancing và Throttling. Ngoài ra các dữ liệu này còn giúp quản trị mạng điều chỉnh lại các quy tắc kiểm soát traffic ra vào mạng của mình.
* **Packet Traceback**: bằng cách dùng kỹ thuật Traceback ta có thể truy ngược lại vị trí của Attacker (ít nhất là subnet của attacker). Từ kỹ thuật Traceback ta phát triển thêm khả năng Block Traceback từ attacker khá hữu hiệu.
* **Bevent Logs:** Bằng cách phân tích file log sau cuộc tấn công, quản trị mạng có thể tìm ra nhiều manh mối và chứng cứ quan trọng.
  1. **Kết luận**
* Mô hình hệ thống cần phải được xây dựng hợp lý, tránh phụ thuộc lẫn nhau quá mức. Bởi một bộ phận gặp sự cố sẽ làm ảnh hưởng tới toàn bộ hệ thống.
* Thiết lập mật khẩu mạnh (strong password) để bảo vệ các thiết bị mạng và các nguồn tài nguyên quan trọng khác.
* Thiết lập các mức xác thực đối với người sử dụng cũng như các nguồn tin trên internet. Đặc biệt, nên thiết lập chế độ xác thực khi cập nhật các thông tin định tuyến giữa các router.
* Liên tục cập nhật, nghiên cứu, kiểm tra để phát hiện các lỗ hổng bảo mật và có biện pháp khắc phục kịp thời. Sử dụng các biện pháp kiểm tra hoạt động hệ thống một cách liên tục để phát hiện ngay những hành động bất thường.
* Nếu bị tấn công do lỗi của phần mềm hay thiết bị thì nhanh chóng cập nhật các bản sửa lỗi cho hệ thống hoặc thay thế.

**VI. Demo tấn công và phòng thủ DOS**

1. **Tấn công bằng Slowloris**

Slowloris là một cuộc tấn công lớp ứng dụng hoạt động bằng cách sử dụng các yêu cầu HTTP một phần. Các chức năng tấn công bằng cách mở các kết nối đến một máy chủ Web được nhắm mục tiêu và sau đó giữ cho các kết nối đó mở miễn là có thể.

**1.1 Sơ đồ bài lap:**

Web server:

* OS: Debian
* IP: 192.168.3.2

Attack:

* OS: Ubuntu
* IP: 192.168.3.3

Client:

* OS: Windows XP
* IP: 192.168.3.10

**1.2 Cài đặt tool để tấn công trên máy Attack**

Yêu cầu:

* Có môi trường python3
* Cài đặt pip3

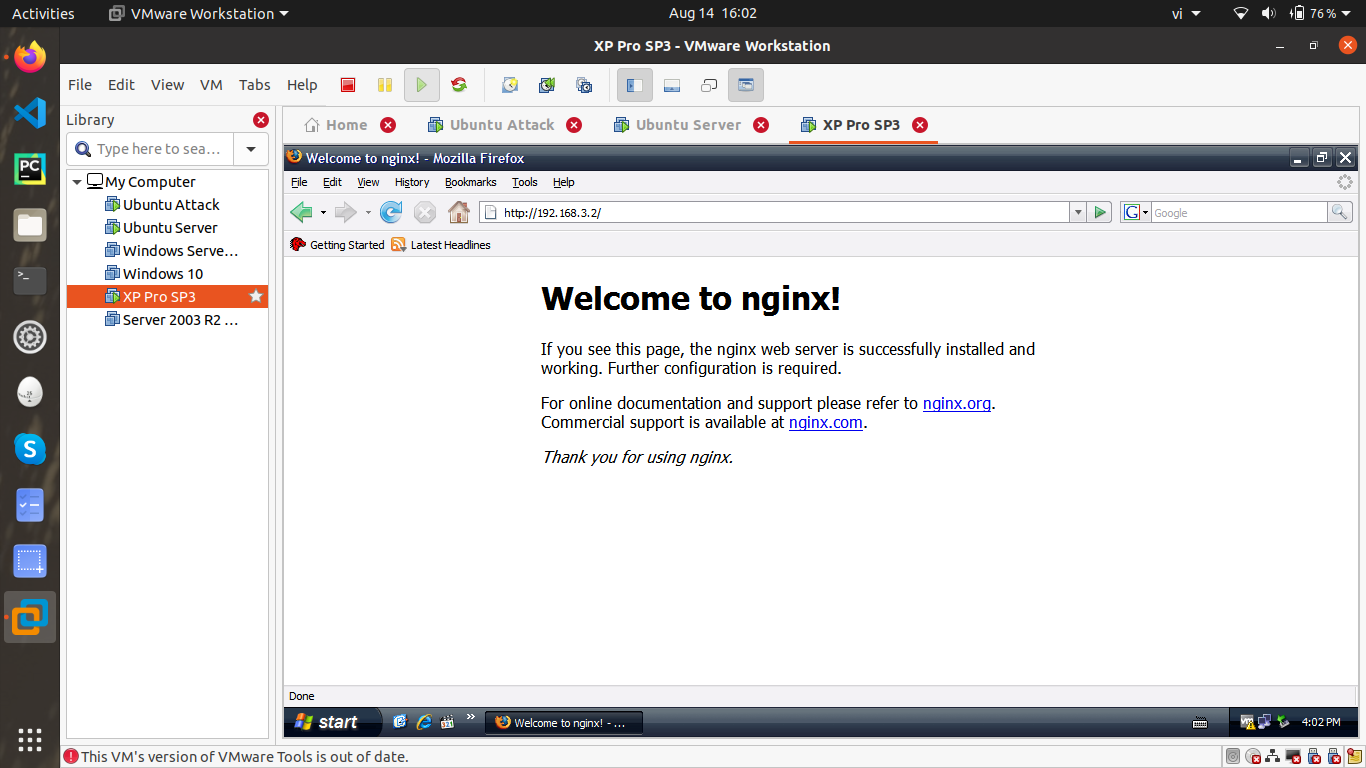
Lệnh để cài đặt slowloris

* sudo pip3 install slowloris
* slowloris 192.168.3.2 -s 2000

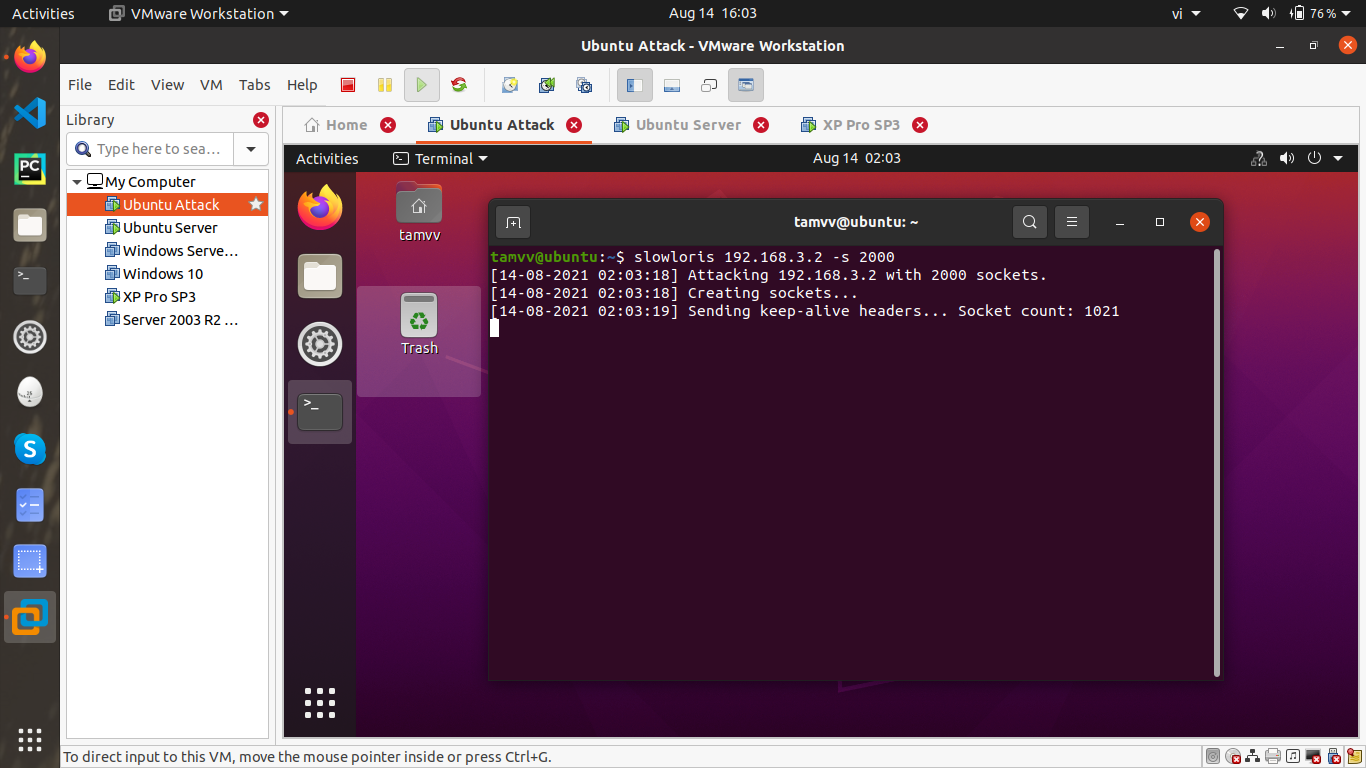
Một số arguments:

1. -s, --port: Số lượng sockets dùng để gửi tới server, mặc định 150
2. -p, --sockets: Port của web server, mặc định 80
3. --https: Sử dụng https cho requests
4. --sleeptime: Thời gian gửi giữa các requests

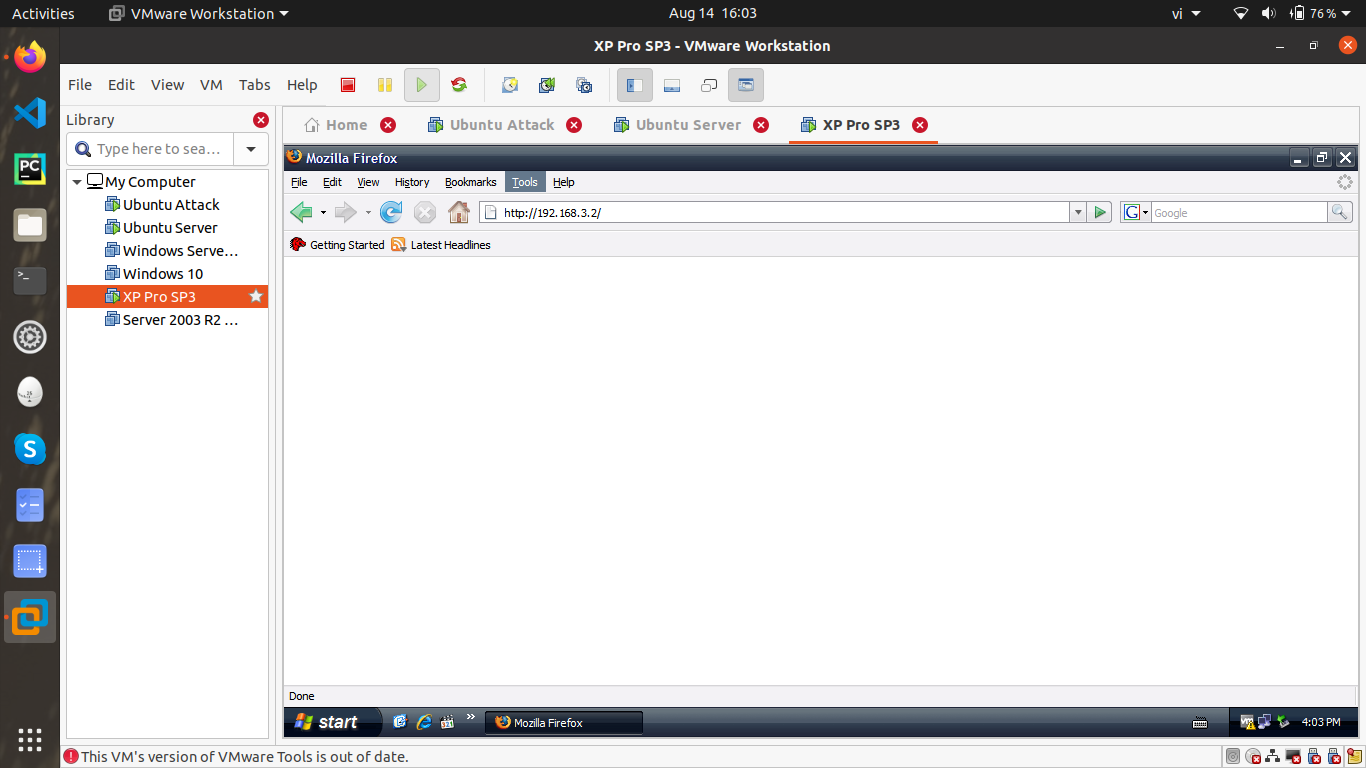
**1.3 Kết quả**



*Trước khi bị tấn công, client vẫn có thể vào bình thường.*



*Tấn công server bằng slowloris*



*Client không thể truy cập vào trang web.*

**2. Bảo vệ server bằng ufw**

**2.1 Cấu hình ufw trên Web server**

Cài đặt ufw:

* sudo apt install ufw

Enable ufw:

* sudo ufw enable

Mở cổng http:

* sudo ufw allow http

Cấu hình script bằng các mở file /etc/ufw/before.rules và chèn đoạn script dưới đây vào trước dòng # End required lines:

# Limit to 20 concurrent connections on port 80/443 per IP

-A ufw-before-input -p tcp --syn --dport 80 -m connlimit --connlimit-above 20 -j DROP

-A ufw-before-input -p tcp --syn --dport 443 -m connlimit --connlimit-above 20 -j DROP

# Limit to 20 connections on port 80/443 per 2 seconds per IP

-A ufw-before-input -p tcp --dport 80 -i eth0 -m state --state NEW -m recent --set

-A ufw-before-input -p tcp --dport 80 -i eth0 -m state --state NEW -m recent --update --seconds 2 --hitcount 20 -j DROP

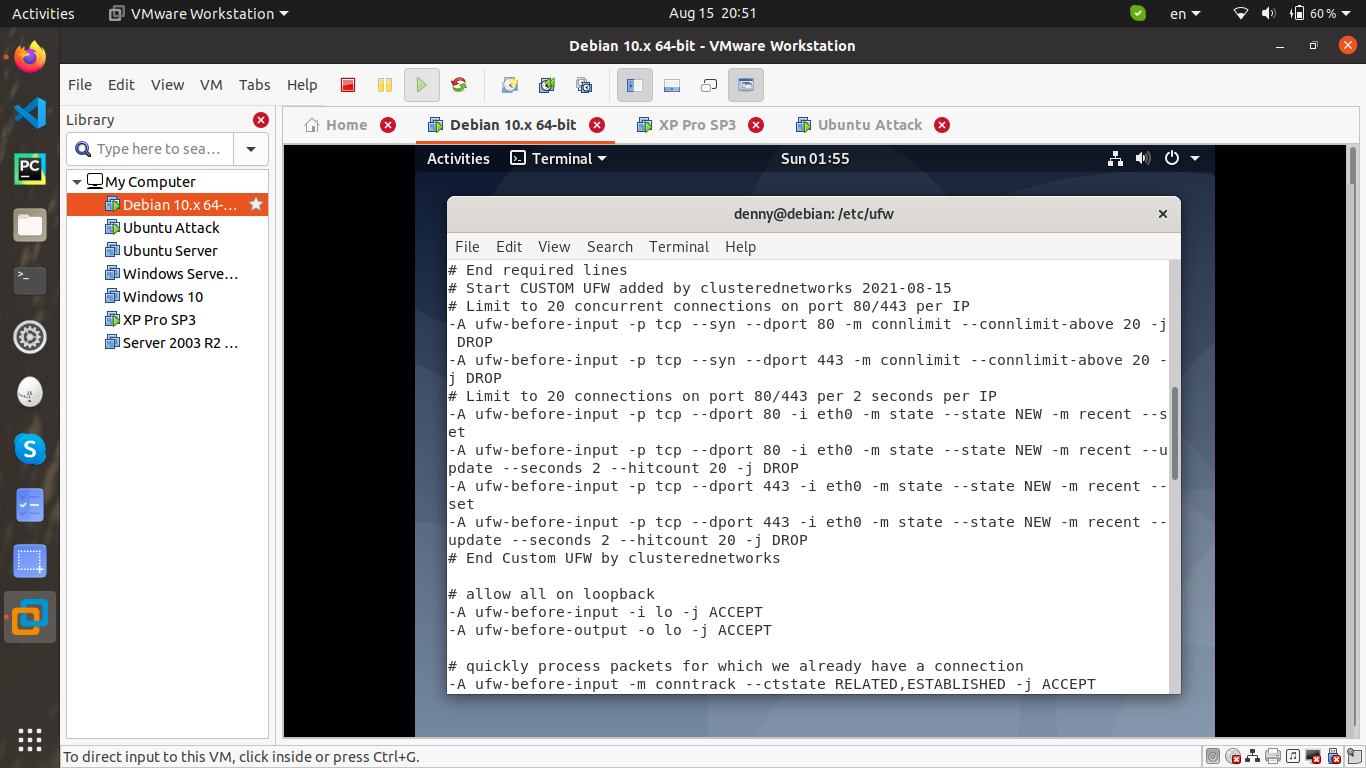
-A ufw-before-input -p tcp --dport 443 -i eth0 -m state --state NEW -m recent --set

-A ufw-before-input -p tcp --dport 443 -i eth0 -m state --state NEW -m recent --update --seconds 2 --hitcount 20 -j DROP

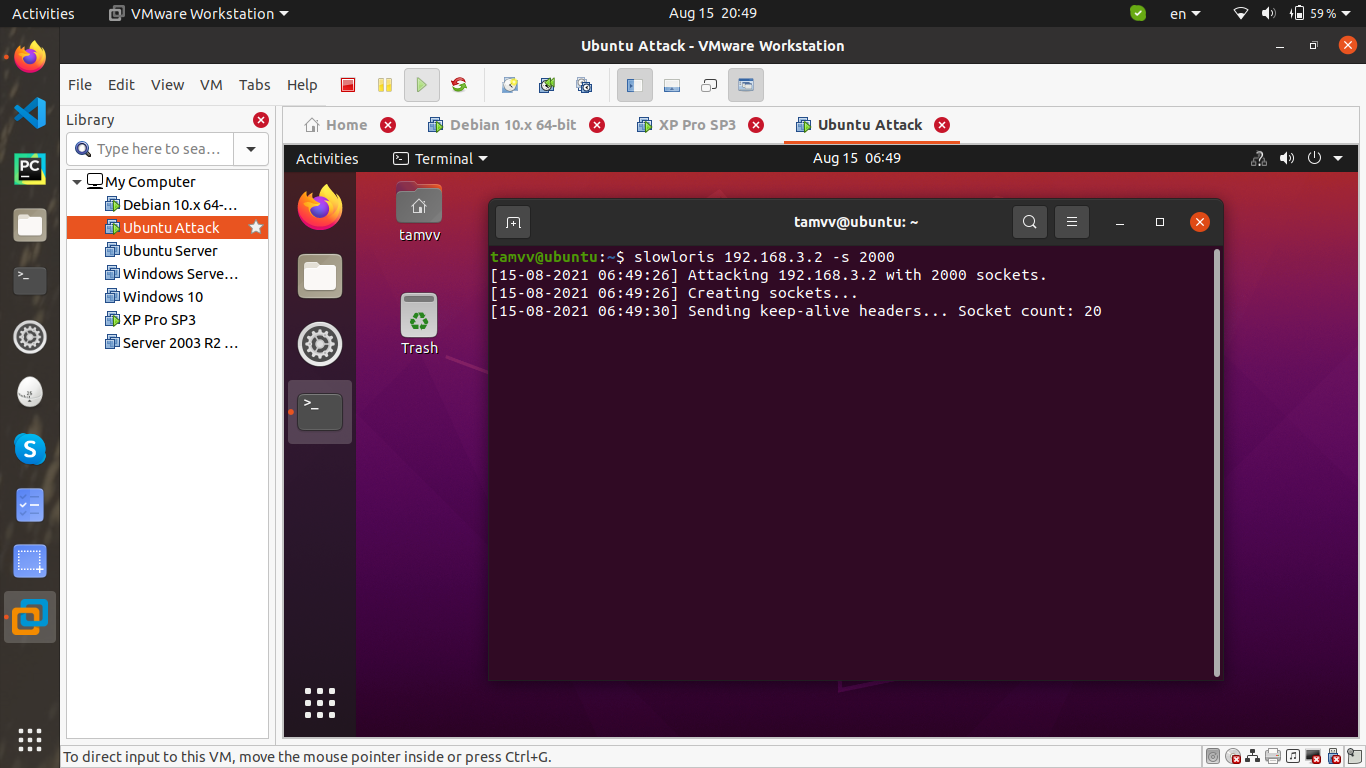
Reload ufw:

* sudo ufw reload

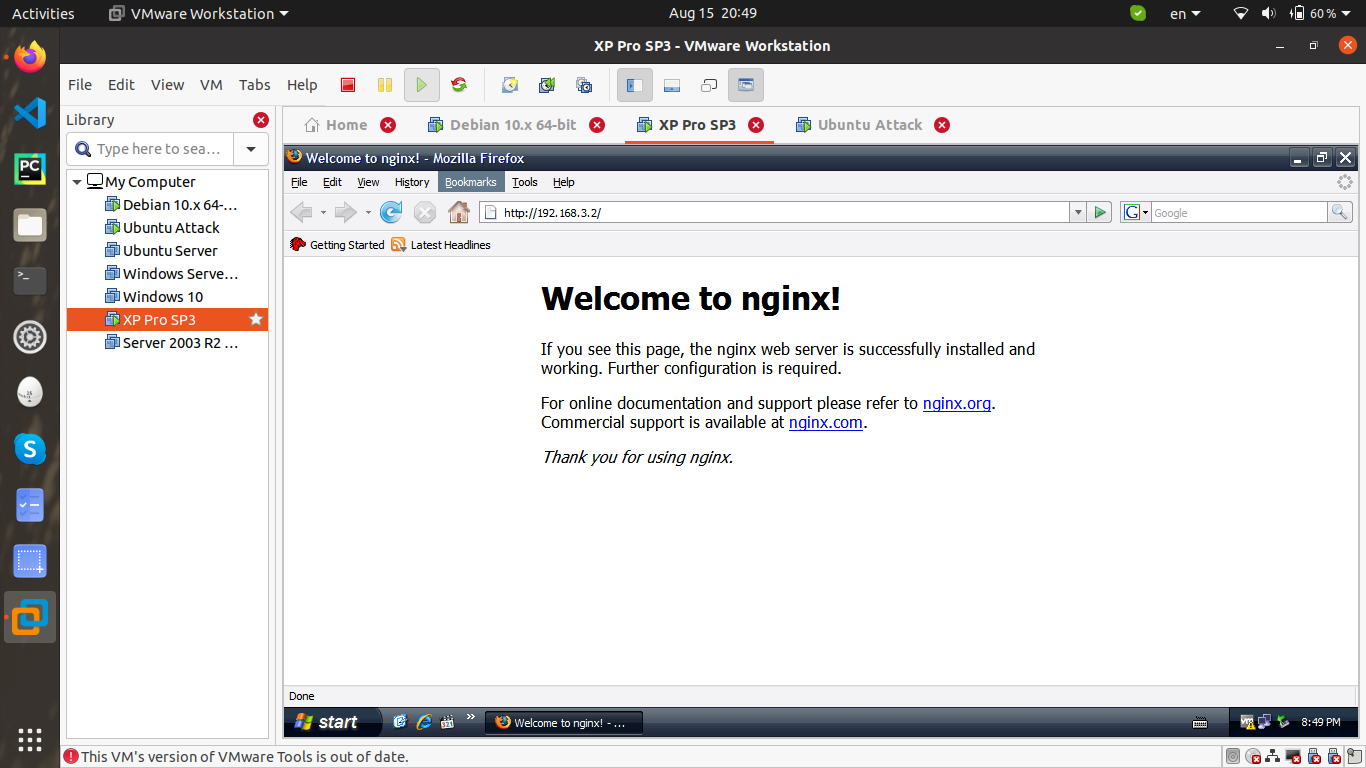
**2.2 Kết quả**



*Config ufw ở server để chống DOS.*



*Tấn công server bằng slowloris*



*Client vẫn có thể truy cập vào trang web.*