| | |
|---|---|
| **Bắt đầu vào lúc** | Thứ ba, 11 Tháng 4 2023, 1:58 PM |
| **Trạng thái** | Đã kết thúc |
| **Kết thúc lúc** | Thứ ba, 11 Tháng 4 2023, 2:46 PM |
| **Thời gian thực hiện** | 47 phút 59 giây |
| **Điểm** | 28,1/50,0 |
| **Điểm** | **5,6** trên 10,0 (**56**%) |

**Câu hỏi 1** Hoàn thành

Trong APT, C&C server có nhiệm vụ ...

- [ ] a. Kết nối với backdoor để nhận lệnh, tải về và cài đặt các module của mã độc
- [x] b. Gửi các module của mã độc đến mục tiêu thông qua backdoor
- [ ] c. Ra lệnh cho mã độc tại mục tiêu hành động
- [ ] d. Tiếp nhận các thông tin do mã độc đánh cắp được từ mục tiêu
- [x] e. Thường đặt trên các server ở nước thứ 3

**Câu hỏi 2** Hoàn thành

Yêu cầu đầu tiên đặt ra với Passive attack là gì?

- (•) a. Đánh cắp được thông tin
- ( ) b. Không bị lộ
- ( ) c. Phân tích lưu lượng thành công
- ( ) d. Tìm được Clear Text password

**Câu hỏi 3** Hoàn thành

Mô tả nào đúng về DoS và DDoS?

- ( ) a. Lưu lượng tấn công DDoS hướng tới nhiều máy trạm khác nhau trong mạng LAN của nạn nhân
- ( ) b. Chỉ có DoS hướng đến mục tiêu làm tê liệt dịch vụ mạng còn DDoS nhằm mục tiêu khác
- (•) c. DoS chỉ sử dụng một vài máy còn DDoS khống chế rất nhiều máy làm công cụ tấn công
- ( ) d. Lưu lượng tấn công DoS chỉ phát sinh từ máy của tin tặc

**Câu hỏi 4** Hoàn thành

Reverse engineering là việc ...

- ( ) a. tấn công mạng bằng những kỹ năng xã hội như thuyết phục, dụ dỗ, dò hỏi
- (•) b. tìm ra cơ chế hoạt động của một phần mềm qua việc phân tích mã nguồn
- ( ) c. dịch mã nguồn thành ngôn ngữ máy

TRƯỜNG ĐẠI HỌC SƯ PHẠM HÀ NỘI
HỆ THỐNG ĐÀO TẠO TRỰC TUYẾN

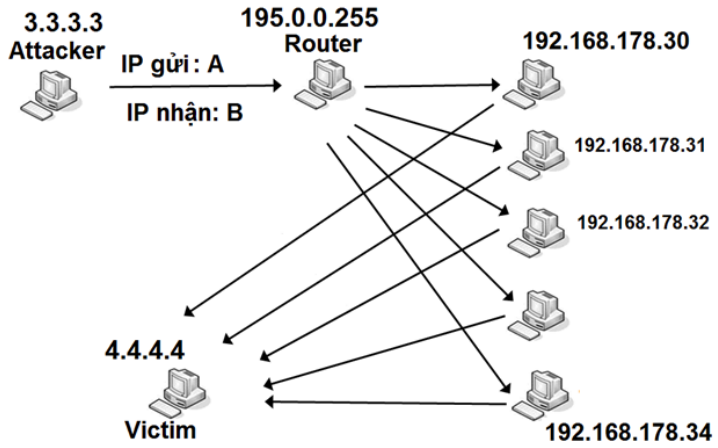
**Câu hỏi 5** Hoàn thành

Thiết lập cấu hình tường lửa để phòng chống SYN flood bằng câu lệnh sau đây đem lại kết quả tích cực gì: #reducing timed out to 30 ?

- a. Ngăn chặn được một phần lưu lượng tấn công khi cuộc tấn công SYN flood xảy ra
- b. Giảm bớt lượng tài nguyên bị tiêu hao trong thời gian bị tấn công SYN flood
- c. Phòng chống được cuộc tấn công SYN flood xuất phát từ những máy ở xa, có tốc độ mạng chậm
- d. Chờ được những client ở xa có tốc độ mạng chậm

**Câu hỏi 6** Hoàn thành

Hình sau mô tả cuộc tấn công SMURT. Gói tin gửi từ hacker tới router của mạng phản xạ ghi địa chỉ gửi là A và địa chỉ nhận là B. Hãy cho biết hai địa chỉ A và B theo thứ tự là những địa chỉ nào?




- a. 195.0.0.255 và 4.4.4.4
- b. 3.3.3.3 và 4.4.4.4
- c. 3.3.3.3 và 195.0.0.255
- d. 4.4.4.4 và 195.0.0.255

**Câu hỏi 7** Hoàn thành

Cơ chế Sandbox bảo mật bằng cách ...

- a. Thực thi các phần mềm cần bảo vệ trong một không gian cách ly khỏi môi trường bên ngoài
- b. Thực hiện cơ chế Blacklisting
- c. Gọi ứng dụng Antivirus
- d. Thực hiện cơ chế Reverse engineering
- e. Hoạt động trong môi trường cách ly được tạo bởi những thiết bị không kết nối ra Internet bên ngoài

**Câu hỏi 8** Hoàn thành

Mô tả nào đúng về DRDoS?

b. Kẻ tấn công mạo danh những máy tính đang bảo trì hoặc ngừng làm việc để trực tiếp gửi rất nhiều gói tin đến nạn nhân

c. Kẻ tấn công mạo danh nạn nhân (địa chỉ gửi là IP của nạn nhân) gửi gói tin SYN tới các server phản xạ dẫn tới hiện tượng nhân băng thông về phía nạn nhân

d. Kẻ tấn công sử dụng đàn botnet để tạo ra cơn bão gói tin

**Câu hỏi 9** Hoàn thành

Mô tả nào về hình thức tấn công từ chối dịch vụ là đúng?

a. Kiểu tấn công LAND gửi tới nạn nhân những gói tin với giá trị offset sai lệch, chồng chéo nhau

b. Nạn nhân không thể lắp ráp 3 gói tin tới đích với giá trị offset như sau. Gói tin thứ nhất: 1-100; gói thứ hai: 201-1000; gói thứ ba: 101-500

c. Kiểu tấn công LAND giả mạo địa chỉ IP của chính nạn nhân để gửi các gói tin tấn công

d. Kiểu tấn công LAND gửi những mảnh khác nhau của gói tin mà nạn nhân không thể lắp ghép lại được

**Câu hỏi 10** Hoàn thành

Mô tả nào sai về kiểu tấn công SYN Flood?

a. Lợi dụng cơ chế "Three way handshake" của giao thức TCP

b. Gói tin được gửi ở bước 3 là ACK, do tin tặc gửi tới nạn nhân

c. Gói tin được gửi ở bước 1 là SYN

d. Gói tin được gửi ở bước 2 là SYN/ACK, do chính nạn nhân gửi đi

**Câu hỏi 11** Hoàn thành

Mô tả nào về hình thức tấn công Ping of Death là sai?

a. Lợi dụng lệnh Ping

b. Gửi gói tin có kích thước bất thường khiến cho máy tính của nạn nhân gặp phải khó khăn khi xử lý

c. Lợi dụng cơ chế bắt tay ba bước của giao thức TCP

d. Hiện nay một số website phòng chống hình thức tấn công Ping of Death bằng cách đặt chế độ từ chối mọi gói tin gửi qua giao thức ICMP

**Câu hỏi 12** Hoàn thành

Đâu là xác thực 2 bước trong các phép kiểm tra sau đây?

a. Name - phone number

b. mã OTP - số PIN

c. Mật khẩu - Vân tay

d. Name - Password

e. mống mắt - giọng nói

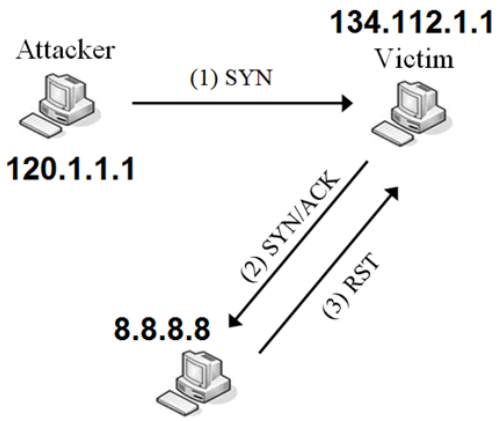
**Câu hỏi 13** Hoàn thành

Sâu Stuxnet được sử dụng trong hình thức tấn công nào?

b. Passive attack
c. DOS
d. Phishing
e. DDOS

**Câu hỏi 14** Hoàn thành

Hình sau mô tả cuộc tấn công SYN Flood trong đó attacker gửi gói SYN tới nạn nhân, gói tin này ghi địa chỉ trạm gửi là gì?




a. 120.1.1.1
b. 8.8.8.8
c. 192.168.1.1
d. 134.112.1.1

**Câu hỏi 15** Hoàn thành

Attacker gửi gói tin nào tới nạn nhân để thực hiện cuộc tấn công SYN Flood?

a. SYN/ACK
b. SYN
c. ACK
d. RST

**Câu hỏi 16** Hoàn thành

Mô tả nào về Passive attack là sai?

a. Kết quả thu được là các thông tin xác thực hoặc file dữ liệu
b. Một ví dụ là hình thức tấn công SMURT
c. Là tiền đề cho các bước tấn công tiếp theo
d. Thà không đánh cắp được dữ liệu chứ nhất định phải đảm bảo nạn nhân không hay biết

**Câu hỏi 17** Hoàn thành

a. Do nhân viên trong cơ quan tiến hành hoặc tiếp tay
b. Một ví dụ là vụ việc của Edward Snowden
c. có thể là một bước trong chiến dịch APT
d. Luôn thuộc loại Passive attack

**Câu hỏi 18** Hoàn thành

Mô tả nào Sai về Buffer overflow attack?

a. Lợi dụng lỗi tràn bộ đệm khi thực hiện chương trình
b. Được thiết kế để thực hiện tấn công DOS
c. Được thiết kế một cách đặc biệt để thực thi đoạn mã độc hoặc phá hoại, khiến một việc thực thi một phần mềm bị trục trặc
d. Ghi đè lên một ô nhớ nhằm thay đổi địa chỉ trả về để tái định hướng tới đoạn mã độc
e. Gây ra một thao tác truy nhập bộ nhớ nguy hiểm

**Câu hỏi 19** Hoàn thành

Đoạn lệnh kèm theo được đánh số thứ tự để tiện theo dõi. Dòng lệnh nào có khả năng gây ra lỗi Buffer overflow?

```
1.  int main(int argc, char *argv[]) {
2.  char buffer[8];
3.  if (argc < 2)  {
4.  fprintf(stderr, "USAGE: %s string\n", argv[0]);
5.  return 1;  }
6.  strcpy(buffer, argv[1]);
7.  return 0;
8.  }
```

a. 6
b. 7
c. 5
d. 4

**Câu hỏi 20** Hoàn thành

Trong hình thức tấn công APT, chữ P có nghĩa là ...

a. Kiên trì
b. Dai dẳng
c. Công khai
d. Bảo vệ
e. Dự án

Mô tả nào đúng về Social engineering?

- a. Sử dụng C&C server
- b. Sử dụng kỹ năng IT
- c. Sử dụng mã độc Trojan
- d. Sử dụng kỹ năng lập trình
- e. Được kẻ gian sử dụng trong cuộc gọi điện thoại lừa đảo

**Câu hỏi 22** Hoàn thành

Mô tả nào sai về hình thức tấn công DoS?

- a. Có thể lợi dụng một đặc điểm nào đó của giao thức mạng, điển hình là SYN Flood
- b. Có thể hướng tới việc vắt kiệt băng thông mạng của nạn nhân
- c. Hiện nay tin tặc chỉ dùng một server duy nhất có công suất lớn để gửi rất nhiều gói tin làm nghẽn băng thông của nạn nhân
- d. Có thể nhằm vào lớp ứng dụng, cụ thể là các phần mềm chạy trên Web server của nạn nhân như IIS, Apache

**Câu hỏi 23** Hoàn thành

Attacker gửi gói tin tới nạn nhân để thực hiện cuộc tấn công SYN Flood. Địa chỉ gửi trong header của gói tin đó không thể là ...

- a. một địa chỉ đã ngừng hoạt động
- b. một địa chỉ của máy tính đang được bảo trì
- c. một địa chỉ chưa cấp phát
- d. một địa chỉ đang hoạt động

**Câu hỏi 24** Hoàn thành

Hình thức tấn công APT ...

- a. Thiết lập trung tâm điều khiển và C&C server
- b. Thiết lập host trung gian để ra lệnh cho mã độc
- c. Gửi email đính kèm file chứa mã độc hoặc đường link chứa backdoor
- d. Sử dụng Social Engineering để lừa gạt, khai thác thông tin
- e. Xóa dấu vết bằng cách gửi dữ liệu đánh cắp được cho C&C server

**Câu hỏi 25** Hoàn thành

Hình thức tấn công DOS và APT có liên quan gì?

- a. APT sử dụng DOS để đánh cắp thông tin
- b. DOS sử dụng APT để khai thác thông tin về mục tiêu
- c. APT sử dụng DOS để tạo ra Backdoor
- d. APT sử dụng DOS để đánh lạc hướng
- e. DOS sử dụng APT để làm tê liệt hệ thống

**Câu hỏi 26** Hoàn thành

Blacklist là ...

- a. Danh sách địa chỉ mà mã độc sẽ lây lan thông qua việc gửi email
- b. Danh sách được ghi nhận bởi các tổ chức chống thư rác, chuyên thống kê những server phát tán thư rác
- c. Máy chủ phát tán mã độc
- d. Danh sách những địa chỉ IP bị nghi ngờ
- e. C&C server

**Câu hỏi 27** Hoàn thành

Hình thức tấn công APT không có tính chất nào sau đây?

- a. Mã hóa dữ liệu rồi đòi tiền chuộc
- b. Đánh cắp dữ liệu
- c. Xóa file
- d. Gửi email chứa bản sao mã độc đến mọi địa chỉ email có liên quan đến mục tiêu
- e. Phá hoại hoạt động của hệ thống

**Câu hỏi 28** Hoàn thành

Hình thức tấn công APT có thể ...

- a. Thực hiện footprinting để kết nối lên C&C server
- b. Sử dụng C&C server để đánh lạc hướng
- c. Cài đặt cửa hậu (backdoor)
- d. Cố gắng lây nhiễm malware vào mục tiêu

**Câu hỏi 29** Hoàn thành

Mô tả nào sai về hình thức tấn công DoS?

- a. Hệ thống không thể nhận dạng những gói tin của tin tặc gửi tới nhằm làm nghẽn băng thông
- b. Hệ thống có thể nhận dạng những gói tin DoS của tin tặc gửi tới vì chúng chứa những signature đặc trưng của mã độc
- c. Công cụ tấn công chỉ là những phần mềm bình thường mà ai cũng sử dụng hàng ngày như trình duyệt
- d. Hoạt động tấn công của tin tặc được hệ thống ưu tiên phục vụ vì hiểu nhầm là các yêu cầu trao đổi từ khách hàng

**Câu hỏi 30** Hoàn thành

Sau khi gõ lệnh ipconfig /all tại cửa sổ lệnh, kết quả hiển thị như sau:

Ethernet adapter:

Physical Address. . . . . : B4-2E-99-76-63-3D

IPv4 Address. . . . . : 192.168.1.7

Subnet Mask . . . . . : 255.255.255.0

DHCP Server . . . . . : 192.168.1.1

Trong trường hợp này địa chỉ MAC của máy là gì?

- a. 255.255.255.0
- b. 192.168.1.1
- c. B4-2E-99-76-63-3D
- d. 192.168.1.7

**Câu hỏi 31** Hoàn thành

Spam traps không phải là ...

- a. Những địa chỉ email được nhúng trong các trang web, nhúng vào danh sách khách hàng để phát hiện địa chỉ IP chuyên phát tán spam mail
- b. Có thể nhầm lẫn, khiến hoạt động của một cá nhân hay tổ chức bị ảnh hưởng
- c. Thư rác
- d. Những địa chỉ email cũ của nhân viên đã thôi việc, được dùng để phát hiện những địa chỉ chuyên phát tán spam mail
- e. Những địa chỉ email được các tổ chức chống thư rác sử dụng để phát hiện những địa chỉ phát tán spam mail

**Câu hỏi 32** Hoàn thành

Mô tả nào về hình thức tấn công Từ chối dịch vụ là sai?

- a. Đầu tư thêm chi phí để nâng cấp cấu hình máy chủ, thiết bị và đường truyền cũng không giúp gì cho việc đối phó với DoS
- b. Hình thức tấn công từ chối dịch vụ kiểu cổ điển Denial of Service, viết tắt là DoS, dùng một máy chủ công suất lớn liên tục gửi truy vấn tới mục tiêu khiến nó bị tắc nghẽn
- c. Cài mã độc vào một website có nhiều người xem hàng ngày để dễ dàng lây nhiễm mã độc cho máy tính của họ
- d. Cài mã độc vào một website có nhiều người xem hàng ngày để khống chế và huy động máy tính của họ tham gia cuộc tấn công từ chối dịch vụ

**Câu hỏi 33** Hoàn thành

Đối với người dùng Nguyễn Văn An sinh ngày 01/01/2001, mật khẩu nào sau đây là mật khẩu mạnh có thể sử dụng được?

- a. mat_khau_hoa_hong
- b. Chieu*tren*pho*vang!285
- c. hoa_hong_01012001
- d. password_ hoa_hong_do_tham

**Câu hỏi 34** Hoàn thành

Mô tả nào đúng về mục đích của hình thức tấn công DOS?

- a. Thường kéo dài trong nhiều ngày
- b. Cướp quyền điều khiển hệ thống mạng của nạn nhân
- c. Khiến cho nạn nhân không thể cung cấp dịch vụ mạng

**Câu hỏi 35** Hoàn thành

Trong APT, footprinting là quá trình ...

- a. Tìm kiếm thông tin về blacklist
- b. Khám phá các thông tin về mục tiêu cần bảo vệ
- c. Khám phá các thông tin về mục tiêu cần tấn công
- d. Tìm kiếm thông tin về backdoor
- e. Ở giai đoạn chuẩn bị, nhưng thường chiếm nhiều thời gian hơn các giai đoạn tiếp theo

**Câu hỏi 36** Hoàn thành

Mô tả nào về Phishing attack là sai?

- a. Mục đích là tìm cách dụ dỗ người dùng gõ các thông tin xác thực
- b. Hacker xây dựng những trang web lừa đảo trông "giống hệt" như các trang web phổ biến để người dùng click vào đó
- c. Hacker gửi nhiều gói tin ICMP làm tắc nghẽn băng thông
- d. Hacker xây dựng những trang web lừa đảo có đường link tương tự trang web thông dụng để khiến người dùng nhầm lẫn

**Câu hỏi 37** Hoàn thành

Mô tả nào đúng về Phising?

- a. Không xác định trước được mục tiêu tấn công
- b. Sử dụng Social engineering
- c. Phishing email thường có nội dung hấp dẫn
- d. Nhắm vào một mục tiêu định trước

**Câu hỏi 38** Hoàn thành

Thiết lập cấu hình tường lửa để phòng chống SYN flood bằng câu lệnh sau đây đem lại kết quả tích cực gì: # limits incoming packets

- a. Giảm bớt lượng tài nguyên bị tiêu hao trong thời gian bị tấn công SYN flood
- b. Ngắt kết nối mạng khi cuộc tấn công SYN flood bắt đầu xảy ra
- c. Phòng chống được cuộc tấn công Insider attack
- d. Làm gia tăng số lượng kết nối có thể tiếp nhận

**Câu hỏi 39** Hoàn thành

Mô tả nào về zero-day attack là sai?

- a. Có cả một thị trường chợ đen mua bán lỗ hổng bảo mật zero-day
- b. Khai thác những lỗ hổng bảo mật chưa được công bố hoặc chưa được vá

**Câu hỏi 40** Hoàn thành

Mô tả nào sai về tấn công mật khẩu?

- a. Có nhiều phần mềm công cụ để thực hiện Dictionary Attack
- b. Dictionary attack: thử những mật khẩu tổ hợp từ những thông tin đánh cắp được
- c. Brute force: thử tất cả các chuỗi mật khẩu có thể
- d. Brute Force: tin tặc thử các mật khẩu mà hắn đánh cắp được từ nạn nhân

**Câu hỏi 41** Hoàn thành

Đoạn lệnh kèm theo được đánh số thứ tự để tiện theo dõi. Dòng lệnh nào có khả năng gây ra lỗi Buffer overflow?

```
1.  #include <stdio.h>
2.  #include <string.h>
3.  int main(int argc, char *argv[]) {
4.  char buffer[10];
5.  if (argc < 2)  {
6.  fprintf(stderr, "USAGE: %s string\n", argv[0]);
7.  return 1;  }
8.  strcpy(buffer, argv[1]);
9.  buffer[sizeof(buffer) - 1] = '\0';
10. return 0;
11. }
```

- a. 9
- b. 8
- c. 6
- d. 4

**Câu hỏi 42** Hoàn thành

Mô tả nào đúng về dấu hiệu cho phép nhận dạng một Phishing email?

- a. Địa chỉ gửi thường là các email công vụ
- b. Địa chỉ nhận thường ghi chính xác họ tên, giới tính của người nhận
- c. Title thường hấp dẫn, cuốn hút
- d. Địa chỉ gửi thường là  các email miễn phí

**Câu hỏi 43** Hoàn thành

Attacker A gửi gói SYN tới nạn nhân B để thực hiện cuộc tấn công SYN Flood. Gói tin này mạo danh một máy

b. C sẽ gửi gói tin ACK cho B
c. B gặp bất lợi
d. A gặp bất lợi

**Câu hỏi 44** Hoàn thành

zero-day là ...

a. lỗ hổng bảo mật
b. lỗ hổng bảo mật chưa được vá
c. lỗ hổng bảo mật chưa được công bố
d. danh sách các lỗ hổng bảo mật chưa được công bố

**Câu hỏi 45** Hoàn thành

Mô tả nào đúng về Captcha?

a. Là những phép thử cho phép phân biệt đối tượng đang tương tác là con người hay phần mềm tự động
b. Là những phép thử do con người tạo ra, chỉ có con người mới có thể vượt qua
c. Là những phép thử do máy tính tạo ra một cách tự động
d. Là những phép thử do con người tạo ra, máy tính hoàn toàn có thể vượt qua

**Câu hỏi 46** Hoàn thành

Mô tả nào đúng về hình thức tấn công DoS?

a. Attacker có thể cài mã độc vào một website có lượng truy cập lớn để tất cả những người truy cập website đều vô tình tham gia vào cuộc tấn công DoS
b. DDoS dễ bị ngăn chặn và truy bắt vì lưu lượng tấn công chỉ xuất phát từ một địa chỉ IP
c. Hình thức DOS tiến tiến hiện nay là tin tặc chỉ dùng một server duy nhất có công suất lớn để gửi rất nhiều gói tin làm nghẽn băng thông của nạn nhân
d. Hình thức DoS cổ điển là ra lệnh cho mạng các zombie đồng loạt tấn công. Ngày nay hình thức này ít được sử dụng vì dễ bị ngăn chặn là lần vết

**Câu hỏi 47** Hoàn thành

Hình thức tấn công APT có thể ...

a. Thực hiện Sandboxing
b. Nén và gửi dữ liệu đánh cắp được lên host trung gian
c. Chống IDS
d. Thực hiện reverse engineering
e. Thực hiện Blacklisting
f. Thường diễn ra trong khoảng thời gian ngắn, tính bằng phút

**Câu hỏi 48** Hoàn thành

Mô tả nào về xác thực hai nhân tố là sai?

- a. Việc đăng nhập vào Facebook thông qua một thao tác nháy chuột vào ảnh là ví dụ về xác thực 2 lớp
- b. Một ví dụ là việc rút tiền từ máy rút tiền tự động ATM
- c. Tiến hành việc xác thực dựa trên hai yếu tố: những gì người dùng biết và những gì họ xuất trình ra được
- d. Tiếng Anh là Two-factor authentication, còn gọi là Xác thực hai bước

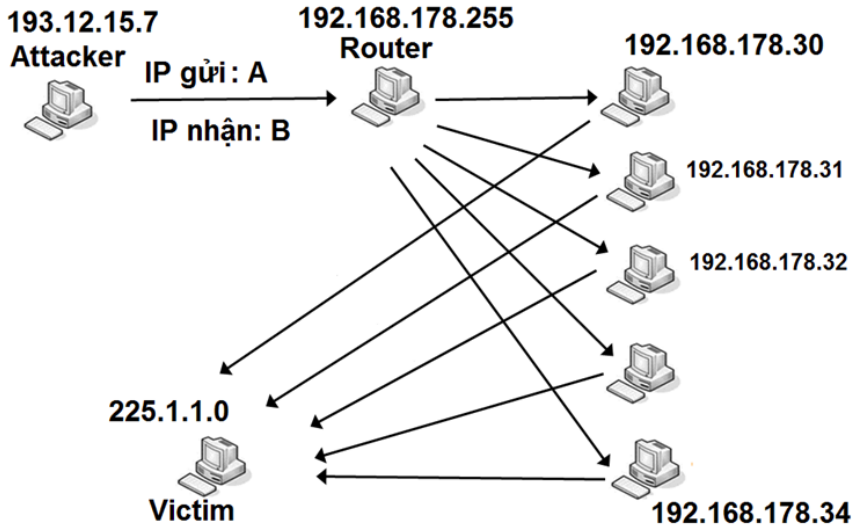
**Câu hỏi 49** Hoàn thành

IDS là ...

- a. Hệ thống phát hiện xâm nhập
- b. Lệnh phát hiện mã độc
- c. Hệ thống chống xâm nhập
- d. Thiết bị phòng chống hoạt động độc lập
- e. Nền tảng tường lửa

**Câu hỏi 50** Hoàn thành

Hình sau mô tả cuộc tấn công SMURT. Gói tin gửi từ hacker tới router của mạng phản xạ ghi địa chỉ gửi là A và địa chỉ nhận là B. Hãy cho biết A là bao nhiêu ?




- a. 192.168.178.255
- b. 193.12.15.7
- c. 225.1.1.0
- d. 192.168.178.30

Hoàn thành xem lại bài kiểm tra

Kiểm tra bù lần 1 cho những sinh viên chưa làm bài

Chuyển tới...