

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA CÔNG NGHỆ THÔNG TIN I



BÁO CÁO BÀI TẬP LỚN

MÔN: PHƯƠNG PHÁP LUẬN NGHIÊN CỨU KHOA HỌC

Giảng viên hướng dẫn:

TS Đinh Thị Hương

Nhóm lớp:

Nhóm 14

Sinh viên thực hiện:

Nguyễn Đức Hoàng

Mã sinh viên:

B17DCAT084

Hà Nội, tháng 12, 2020

MỤC LỤC

| | |
|--|----|
| MỤC LỤC | 2 |
| LỜI NÓI ĐẦU | 3 |
| Câu 1: Trình bày những nội dung chính trong Phần mở đầu của một bài báo khoa học. Phân tích Phần mở đầu một bài báo khoa học theo ngành (chuyên ngành) của anh (chị) để làm minh chứng. | 4 |
| Câu 2: Anh (chị) hiểu thế nào là tính kế thừa trong nghiên cứu khoa học..... | 6 |
| Câu 3: Liệt kê các kiểu trích dẫn khoa học thường được sử dụng. Anh (Chị) hãy sử dụng thẻ References trong Word và tự lập một danh mục tài liệu tham khảo theo chuẩn..... | 6 |
| LỜI CẢM ƠN..... | 10 |

LỜI NÓI ĐẦU

Tất cả mọi hoạt động công việc, học tập hay sáng tạo đều cần yêu cầu phải có sự nghiên cứu kỹ về những khía cạnh của vấn đề mà chúng ta định tham gia. Điều đó góp phần cung cấp lượng lớn tri thức cũng như chỉ ra những thiếu sót của những người đi trước trong lĩnh vực chúng ta quan tâm, qua đó giúp công việc của chúng ta trở nên hiệu quả hơn, mang lại lợi ích to lớn hơn.

Hiểu được tầm quan trọng của điều này, Học viện Công nghệ Bưu chính Viễn thông đã tạo điều kiện cho sinh viên được tham gia vào môn học Phương pháp luận Nghiên cứu Khoa học, từ đó giúp sinh viên hiểu được mình phải làm gì, làm như thế nào, quy trình ra sao trước khi tham gia vào một đề tài Nghiên cứu khoa học, hoặc đơn giản hơn là áp dụng để có những chiến lược trong công việc, trong học tập cũng như đưa ra những định hướng tương lai tốt hơn.

Câu 1: Trình bày những nội dung chính trong Phần mở đầu của một bài báo khoa học. Phân tích Phần mở đầu một bài báo khoa học theo ngành (chuyên ngành) của anh (chị) để làm minh chứng.

- Phần mở đầu của một bài báo khoa học bao gồm những nội dung sau:
 - 1) Lý do nghiên cứu (Tại sao tôi nghiên cứu?).
 - 2) Lịch sử nghiên cứu (Ai đã làm gì?).
 - 3) Mục tiêu nghiên cứu (Tôi sẽ làm gì?).
 - 4) Mẫu khảo sát (Tôi làm ở đâu?).
 - 5) Phạm vi nội dung nghiên cứu (Giới hạn nội dung nghiên cứu).
 - 6) Lựa chọn khoảng thời gian đủ để quan sát biến động của sự kiện (Thời gian đủ để quan sát quy luật biến động của sự kiện, không phải là thời gian làm đề tài).
 - 7) Vấn đề nghiên cứu (Câu hỏi nào đòi hỏi phải trả lời trong nghiên cứu?).
 - 8) Luận điểm khoa học (Giả thuyết khoa học chủ đạo của nghiên cứu).
 - 9) Phương pháp chứng minh giả thuyết.
- Phân tích mở đầu của bài báo “KHẢO SÁT CÁC NỀN TẢNG VÀ KỸ THUẬT XỬ LÝ LOG TRUY CẬP DỊCH VỤ MẠNG CHO PHÁT HIỆN NGUY CƠ MẤT AN TOÀN THÔNG TIN” của tác giả Phạm Duy Lộc, Hoàng Xuân Dậu được đăng trên tạp chí khoa học đại học Đà Lạt tập 8 số 2 năm 2018, chuyên san Khoa học tự nhiên và công nghệ.

1. ĐẶT VẤN ĐỀ

Lý do nghiên cứu

Việc giám sát thu thập, xử lý và phân tích các nhật ký, hay vết truy cập (*access log*, từ đây gọi tắt là *log*) mạng nói chung và các log truy cập các dịch vụ mạng nói riêng là nhiệm vụ không thể thiếu trong các hệ thống giám sát, phát hiện bất thường, phát hiện tấn công, xâm nhập hệ thống và mạng. Từ dữ liệu log thu thập được, qua quá trình xử lý, phân tích, chúng ta có thể trích xuất được các thông tin quan trọng về dấu hiệu, hoặc khả năng xuất hiện của các hành vi truy cập bất thường, các dạng mã độc và các dạng tấn công, xâm nhập. Kết quả phân tích, phát hiện dấu hiệu xuất hiện của các truy cập bất thường, mã độc, tấn công, xâm nhập là đầu vào quyết định việc đưa ra các cảnh báo nguy cơ mất an toàn thông tin đối với hệ thống. Đồng thời, kết quả phân tích, phát hiện cũng là một trong các căn cứ quan trọng hỗ trợ việc đánh giá, lựa chọn và triển khai các giải pháp đảm bảo an toàn phù hợp cho thông tin, hệ thống và các tài nguyên mạng. Vấn đề này càng quan trọng hơn trong bối cảnh an toàn thông tin ở Việt Nam đã và đang trở thành vấn đề nóng được các cơ quan, tổ chức chính phủ, các doanh nghiệp và cả xã hội quan tâm.

Theo Báo cáo An toàn thông tin Việt Nam 2016 (Cục An toàn Thông tin, 2016) thì tình hình an toàn thông tin Việt Nam năm 2016 tiếp tục diễn biến phức tạp. Theo đó, số lượng các cuộc tấn công mạng có chiều hướng tăng so với các năm trước đây, nhất là các tấn công mạng vào hệ thống thông tin của cơ quan nhà nước và các doanh nghiệp lớn. Tấn công mạng tiếp tục tăng về quy mô và số lượng, nhất là các cuộc tấn công từ chối dịch vụ phân tán (*Distributed Denial of Service - DDoS*) và tấn công có chủ đích (*Advanced Persistent Threats - APT*). Điển hình là vụ tấn công mạng vào Tổng Công ty Hàng không Việt Nam vào cuối tháng 7 năm 2016. Nhiều cơ quan, tổ chức khác của nhà nước sau khi được rà soát, kiểm tra, đánh giá an toàn cho hệ thống thông tin cũng đã phát hiện ra nhiều điểm yếu, lỗ hổng, bị lây nhiễm phần mềm độc hại và nguy cơ mất an toàn thông tin là rất lớn.

Báo cáo An toàn thông tin Việt Nam 2016 (Cục An toàn Thông tin, 2016) cũng dự báo tình hình an toàn thông tin Việt Nam trong năm 2017 và những năm tới sẽ tiếp tục diễn biến phức tạp với sự bùng nổ của các thiết bị IoT và sự phát triển mạnh của các dịch vụ trực tuyến trên nền Web/Internet. Do vậy, yêu cầu đảm bảo an toàn cho hệ thống thông tin của các cơ quan tổ chức chính phủ, doanh nghiệp và đảm bảo tính riêng tư của từng người dùng là cấp thiết. Với hệ thống máy chủ cung cấp dịch vụ mạng thiết yếu, như các máy chủ Web và các máy chủ tên miền, việc giám sát phát hiện các truy nhập bất thường và cảnh báo các nguy cơ mất an toàn thông tin là một nội dung đặc biệt quan trọng trong nhóm các giải pháp đảm bảo an toàn thông tin cho hệ thống cung cấp dịch vụ, đảm bảo cho hệ thống có thể hoạt động thông suốt, giảm thiểu thời gian ngừng dịch vụ do sự cố an toàn thông tin.

vụ Web và dịch vụ tên miền. Dựa trên kết quả khảo sát, đánh giá, bài báo đề xuất kiến trúc hệ thống giám sát, hỗ trợ đảm bảo an toàn thông tin cho các cơ quan, tổ chức có quy mô hệ thống mạng và nguồn lực hạn chế. **Mục tiêu nghiên cứu**

Bài báo này trước hết khảo sát, đánh giá các nền tảng, công cụ và các kỹ thuật xử lý, phân tích log truy cập phục vụ phát hiện các hành vi bất thường và nguy cơ mất an toàn thông tin trong các hệ thống cung cấp dịch vụ mạng, bao gồm các hệ thống dịch

91

Phạm vi nội dung nghiên cứu

TẠP CHÍ KHOA HỌC ĐẠI HỌC ĐÀ LẠT [ĐẶC SAN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG]

vụ Web và dịch vụ tên miền. Dựa trên kết quả khảo sát, đánh giá, bài báo đề xuất kiến trúc hệ thống giám sát, hỗ trợ đảm bảo an toàn thông tin cho các cơ quan, tổ chức có quy mô hệ thống mạng và nguồn lực hạn chế.

Phần còn lại của bài báo được bố cục như sau: Mục 2 khảo sát, so sánh các nền tảng và công cụ xử lý, phân tích log truy cập. Mục 3 phân tích các kỹ thuật phát hiện các nguy cơ mất an toàn thông tin dựa trên phân tích log truy cập. Mục 4 là phần nhận xét và đề xuất, và Mục 5 là kết luận của bài báo.

Câu 2: Anh (chị) hiểu thế nào là tính kế thừa trong nghiên cứu khoa học.

Tính kế thừa có ý nghĩa quan trọng về mặt phương pháp nghiên cứu khoa học. Không một công trình nghiên cứu nào bắt đầu từ chỗ hoàn toàn trống không về kiến thức. Mỗi nghiên cứu đều phải kế thừa các kết quả nghiên cứu khác có thể cùng khoa học hoặc các khoa học lân cận và xa.

Câu 3: Liệt kê các kiểu trích dẫn khoa học thường được sử dụng. Anh (Chị) hãy sử dụng thẻ References trong Word và tự lập một danh mục tài liệu tham khảo theo chuẩn.

- Các kiểu trích dẫn khoa học thường được sử dụng:
 - APA (American Psychological Association) là kiểu trích dẫn ra đời năm 1929 bởi một nhóm các nhà tâm lý học, nhân chủng học và quản lý kinh doanh, kiểu trích dẫn này nhấn mạnh vào tên tác giả và thời gian công bố tác phẩm.
 - MLA (Modern Language Association) hiện được cho là kiểu trích dẫn được sử dụng nhiều nhất trong nghiên cứu, đặc biệt là lĩnh vực nhân văn và nghệ thuật. Dưới đây là hướng dẫn cơ bản hình thức trích dẫn này trong phiên bản mới nhất của MLA Handbook (xuất bản lần thứ 8).
 - Havard là hình thức trích dẫn khá giống với APA, thường được dùng trong các ngành nhân văn.

- Chicago và Turabian là kiểu trích dẫn được Chicago University Press phát hành từ năm 1906. Hình thức trích dẫn này có 2 loại cơ bản là kiểu dùng cho danh mục tham khảo (thường dùng trong các ngành nhân văn) và kiểu dùng cho trích dẫn trong văn bản, sau đó trích dẫn trong danh mục (thường dùng trong các ngành khoa học xã hội, vật lý, tự nhiên).
 - IEEE (Institute for Electrical and Electronics Engineers) là kiểu trích dẫn của tổ chức cùng tên, gồm các nhánh về kỹ thuật, khoa học máy tính và công nghệ thông tin. Kiểu trích dẫn này gồm trích dẫn trong văn bản với các con số nằm trong ngoặc vuông và xếp thứ tự trong danh mục cũng theo số chữ không phải bằng chữ cái.
 - Vancouver là kiểu trích dẫn cũng sử dụng số như IEEE và thường được dùng trong các nghiên cứu khoa học và y tế. Một số nguyên tắc quan trọng khi sử dụng kiểu trích dẫn này:
 - Số thứ tự trong danh mục tham khảo lần lượt theo thứ tự xuất hiện trong bài, nếu bài viết lặp lại trích dẫn thì dùng lại số trước đó.
 - Dùng số Ả rập (1 - 9) và có thể dùng với ngoặc vuông, ngoặc tròn hoặc chỉ số trên, miễn là phải đồng nhất.
- Chuẩn APA:

Tài liệu tham khảo

- Joshua J. Drake, Zach Lanier, Collin Mulliner, Pau Oliva Fora, Stephen A. Ridley, Georg Wicherski. (2014). *Android Hacker's Handbook*. Wiley.
- Le, N. V. (n.d.). *Mobile App Security - Overview*. - Sun* Cyber Security Research.
- Meyer, R. (2008). Attacks on Web Applications. In *Detecting Attacks on Web Applications from Log Files*.
- Nguyễn Thị Kim Chi, Phạm Thị Kim Ngọc. (2018). Các yếu tố ảnh hưởng đến khả năng thích ứng của cán bộ quản lý trong doanh nghiệp viễn thông Việt Nam. *TC Công Thương / Bộ Công thương, số 13*, 125-131.
- Nhật, N. L. (2020, 3 13). Retrieved from [jstic.ptit.edu.vn](http://jstic.ptit.edu.vn/index.php/jstic/article/view/236):
<http://jstic.ptit.edu.vn/index.php/jstic/article/view/236>
- Thanh, P. V. (2018). Các nhân tố ảnh hưởng đến chi phí môi trường theo quan điểm mức độ nhạy cảm với môi trường của doanh nghiệp. *TC Kế toán và Kiểm toán / Hội KT&KT Việt Nam*, 53-56.
- Watchfire. (n.d.). *HTTP Request Smuggling*.

- Chuẩn MLA:

Tài liệu tham khảo

- [1] P. V. H. Thanh, "Các nhân tố ảnh hưởng đến chi phí môi trường theo quan điểm mức độ nhạy cảm với môi trường của doanh nghiệp," *TC Kế toán và Kiểm toán / Hội KT&KT Việt Nam*, pp. 53-56, 2018 .
- [2] Nguyễn Thị Kim Chi, Phạm Thị Kim Ngọc, "Các yếu tố ảnh hưởng đến khả năng thích ứng của cán bộ quản lý trong doanh nghiệp viễn thông việt nam," *TC Công Thương / Bộ Công thương, số 13*, pp. 125-131, 2018.
- [3] Joshua J. Drake, Zach Lanier, Collin Mulliner, Pau Oliva Fora, Stephen A. Ridley, Georg Wicherski, *Android Hacker's Handbook*, Wiley, 2014.
- [4] Watchfire, HTTP Request Smuggling.
- [5] N. V. Le, Mobile App Security - Overview, - Sun* Cyber Security Research.
- [6] R. Meyer, "Attacks on Web Applications," in *Detecting Attacks on Web Applications from Log Files*, 2008.
- [7] N. L. Nhật, 13 3 2020. [Online]. Available: <http://jstic.ptit.edu.vn/index.php/jstic/article/view/236>.

- Chuẩn IEEE:

Tài liệu tham khảo

- Joshua J. Drake, Zach Lanier, Collin Mulliner, Pau Oliva Fora, Stephen A. Ridley, Georg Wicherski. *Android Hacker's Handbook*. Wiley, 2014.
- Le, Nghia Van. *Mobile App Security - Overview*. - Sun* Cyber Security Research, n.d.
- Meyer, Roger. "Attacks on Web Applications." *Detecting Attacks on Web Applications from Log Files*. 2008.
- Nguyễn Thị Kim Chi, Phạm Thị Kim Ngọc. "Các yếu tố ảnh hưởng đến khả năng thích ứng của cán bộ quản lý trong doanh nghiệp viễn thông việt nam." *TC Công Thương / Bộ Công thương, số 13* (2018): 125-131.
- Nhật, Nguyễn Lương. 13 3 2020. *jstic.ptit.edu.vn*.
<<http://jstic.ptit.edu.vn/index.php/jstic/article/view/236>>.
- Thanh, Phạm Vũ Hà. "Các nhân tố ảnh hưởng đến chi phí môi trường theo quan điểm mức độ nhạy cảm với môi trường của doanh nghiệp." *TC Kế toán và Kiểm toán / Hội KT&KT Việt Nam* (2018): 53-56.
- Watchfire. *HTTP Request Smuggling*. n.d.

LỜI CẢM ƠN

Đầu tiên, em xin gửi lời cảm ơn sâu sắc đến Học viện Công nghệ Bưu chính Viễn thông đã đưa môn học Phương pháp luận Nghiên cứu Khoa học vào trong chương trình giảng dạy. Đặc biệt, em xin gửi lời cảm ơn sâu sắc đến giảng viên bộ môn là cô Đinh Thị Hương đã dạy dỗ, rèn luyện và truyền đạt những kiến thức quý báu cho em trong suốt thời gian học tập kỳ vừa qua. Trong thời gian được tham dự lớp học của cô, em đã được tiếp thu thêm nhiều kiến thức bổ ích, học tập được tinh thần làm việc hiệu quả, nghiêm túc. Đây thực sự là những điều rất cần thiết cho quá trình học tập và công tác sau này của em.

Bộ môn Phương pháp luận Nghiên cứu Khoa học là môn học thú vị, bổ ích và gắn liền với nhu cầu thực tiễn của mỗi sinh viên. Tuy nhiên, vì thời gian học tập trên lớp không nhiều, mặc dù đã cố gắng nhưng chắc chắn những hiểu biết và kỹ năng về môn học này của em còn nhiều hạn chế. Do đó, Bài tiểu luận kết thúc học phần của em khó có thể tránh khỏi những thiếu sót và những chỗ chưa chuẩn xác, kính mong giảng viên bộ môn xem xét và góp ý giúp Bài tiểu luận của em được hoàn thiện hơn.

Em xin chân thành cảm ơn!

Hà Nội, ngày 13 tháng 12 năm 2020

SINH VIÊN

Nguyễn Đức Hoàng

