1. Tóm tắt

Mặc dù các tội phạm mạng phổ biến, công nghệ thông tin và truyền thông (ICT) đã trở thành phương tiện giao tiếp và trao đổi thông tin tiện lợi nhất. Với sự phát triển này, vi phạm bảo mật thông tin hiện nay là một trong những vấn đề phức tạp và thách thức mà các nhà phát triển phần mềm đang đối mặt. Các công cụ đã được phát triển cho mục đích kiểm tra thâm nhập nhằm nâng cao mức độ bảo mật, cũng đã bị những kẻ xâm nhập độc hại sử dụng để truy cập vào thiết bị của chúng ta. Bài báo này nhằm đánh giá hiệu quả của một số công cụ tránh phần mềm diệt virus (AV) được chọn: Avet, Veil 3.0, PeCloak.py, Shellter và Fat Rat, đối với nền tảng Windows. Việc chọn các công cụ này nhằm mục đích kiểm tra cách chúng có thể tạo ra phần mềm độc hại không thể phát hiện đối với các sản phẩm Giải pháp Antivirus tốt nhất hiện tại trên thị trường. Điều này, đến lượt nó, đã tiết lộ các giải pháp AV có hiệu suất tốt nhất trong việc phát hiện phần mềm độc hại có khả năng tránh phát hiện. Bài báo áp dụng thiết kế nghiên cứu thực nghiệm, trong môi trường phòng thí nghiệm ảo với VMware Oracle VirtualBox, bao gồm hai máy (máy tấn công và máy mục tiêu). Kết quả thu được cho thấy tỷ lệ tránh phần mềm diệt virus dao động từ 0% đến 83%. Các công cụ tránh AV Avet và PeCloak.py là tốt nhất, trong khi Kaspersky và Bitdefender antivirus xuất hiện là phần mềm bảo vệ tốt nhất trong việc phát hiện các thủ đoạn tránh phần mềm độc hại.

Từ khóa: Antivirus, Công cụ Tránh, Phần mềm độc hại, Metasploit, Tin tặc.

2. Giới thiệu

Sự phát triển của công nghệ máy tính và internet đã khiến nhiều tổ chức và cá nhân phụ thuộc nặng nề vào các dịch vụ mạng máy tính, chẳng hạn như truy cập vào các trang web, video và âm thanh kỹ thuật số, sử dụng chung ứng dụng và máy chủ lưu trữ, và các dịch vụ liên thông khác (Shrestha, 2012). Ngày nay, hệ thống toàn cầu hóa cho phép các tổ chức hoạt động, hợp tác và chia sẻ tài nguyên thông tin giữa họ nhưng đồng thời cũng khiến họ tiếp xúc với nhiều mối đe dọa cả bên trong và bên ngoài tổ chức. Kết quả là, các tổ chức cần bảo vệ tài nguyên thông tin của họ (Yoo et al., 2017). Các vi phạm bảo mật mạng có thể dẫn đến mất độ tin cậy kinh doanh và năng suất. Trong khi đó, thời gian và lao động liên quan đến việc tái tổ chức các hệ thống bị nhiễm tạo ra chi phí đáng kể (Shrestha, 2012).

Ogeto (2004) lập luận rằng, trong lĩnh vực mạng internet, việc phụ thuộc nặng nề vào máy tính và các công nghệ khác đặt ra một bộ nhu cầu bảo mật mới. Các hệ thống thông tin và mạng ngày càng đối mặt với các mối đe dọa bảo mật từ tin tặc bên trong hoặc bên ngoài mạng và trở thành một trong những vấn đề phức tạp và quan trọng nhất cần quan tâm.

Nikolaos (2018) tin rằng các nhà kiểm tra thâm nhập được thúc đẩy để tham gia và phát triển các công cụ và kỹ thuật tương tự như được sử dụng bởi các tin tặc thực sự, để tấn công hệ thống và tiết lộ các lỗ hổng bảo mật của nó. Điều này thăm dò điểm yếu của hệ thống tổ chức và xác định những gì cần thiết để bảo vệ nó khỏi sự xâm nhập thực sự.

Chuyên môn mạng thường tập trung vào đánh giá bảo mật như một phương tiện quan trọng để hiểu rõ hơn về trạng thái bảo mật hệ thống thông tin. Do đó, kết quả đánh giá là cơ sở quan trọng để xây dựng giải pháp mạng và bảo mật (Johnston & Garcia, 2002). Tuy nhiên, các phương pháp và phương tiện mới cho đánh giá bảo mật mạng đang phát triển và thay đổi mọi lúc và nghiên cứu mới vẫn có thể khai thác cơ hội để lấp đầy khoảng trống với tài liệu hiện tại. Tuy nhiên, tin tặc sử dụng phần mềm độc hại để truy cập vào máy tính mục tiêu qua mạng. Theo thời gian, họ bắt đầu gọi phần mềm độc hại hoặc script là "payload" mà họ sẽ sử dụng chống lại mục tiêu của mình theo cách tương tự như phi công quân sự sử dụng tên lửa chống lại mục tiêu vật lý của họ.

Techopedia (2019) giải thích rằng phần mềm độc hại ngày nay ít có khả năng tích hợp payload gây thiệt hại cho tệp hệ thống; thay vào đó, chúng cho phép backdoor để truy cập máy tính của người dùng và đánh cắp thông tin nhạy cảm. Những payload độc hại này thường được tạo ra bằng cách sử dụng các công cụ khai thác như Core Impact, Canvas và Metasploit Framework.

Có ba kỹ thuật chính được sử dụng trong việc phát hiện phần mềm độc hại bởi phần mềm bảo vệ antivirus, bao gồm Kỹ thuật Dựa trên Chữ ký, Dựa trên Hành vi và Dựa trên Heuristic (Barriga et al., 2017). Trong các cuộc tấn công mạng, bảo vệ Antivirus là một trong những tuyến phòng thủ đầu tiên mà kẻ tấn công đối mặt khi họ cố gắng hack máy tính. Và để tránh phát hiện, những người phát minh công cụ tránh antivirus cũng triển khai nhiều kỹ thuật. Những kỹ thuật này là làm mờ, tấn công tái sử dụng mã, mã hóa, oligomorphism, polymorphism và metamorphism.

Công cụ tránh antivirus được sử dụng bởi cả kẻ tấn công độc hại và nhà kiểm tra thâm nhập. Thực hành được sử dụng bởi các chuyên gia bảo mật để đánh giá sức mạnh bảo mật hệ thống được gọi là kiểm tra thâm nhập. Kiểm tra thâm nhập liên quan đến việc tấn công hệ thống để phát hiện các lỗ hổng có thể bị khai thác bởi tin tặc độc hại. Do đó, kết quả đánh giá là cơ sở quan trọng để xây dựng giải pháp mạng và bảo mật (Johnston & Garcia, 2002). Vì vậy, có nhu cầu đánh giá hiệu quả của các công cụ tránh antivirus được sử dụng bởi kẻ xâm nhập độc hại và nhà kiểm tra thâm nhập tương ứng.

3. Các công cụ liên quan

Để xem xét các nghiên cứu liên quan trước đó, Kalogranis (2018) đã đánh giá bốn (4) công cụ tránh antivirus, chống lại năm (5) sản phẩm phần mềm antivirus trên nền tảng window. Các giải pháp antivirus tốt nhất theo nghiên cứu của ông đã được chọn. Sau đó, tỷ lệ tránh tốt nhất đã được đạt được từ nghiên cứu được thực hiện, trong đó công cụ tránh Avet và Veil đã vượt qua hầu hết các bảo vệ antivirus và được chỉ định là công cụ tránh tốt nhất.

Tương tự, Themelis (2018) đã sử dụng công cụ tránh pyRAT để tự động hóa việc tạo payload thực thi Metasploit và xâm nhập hệ thống mà không bị phát hiện bởi hầu hết các giải pháp antivirus. Trong nghiên cứu của ông, pyRAT đáp ứng tất cả các yêu cầu về khả năng sử dụng

và sử dụng công cụ kiểm tra thâm nhập, được gọi là Metasploit Framework cùng với các tính năng của nó. Công trình trình bày công nghệ pyRAT và cho thấy một cách đơn giản và rõ ràng cách đạt được sự xâm nhập vào hệ thống một cách hiệu quả và bí mật mà không bị bắt bởi hầu hết các antivirus.

Sukwong et al. (2011) đã đánh giá hiệu quả của phần mềm antivirus thương mại. Họ đã đưa mỗi phần mềm độc hại mới mà họ thu thập vào sáu (6) quét AV thương mại nổi tiếng sau: i. Avast 4.8 Professional v.4.8.1335, ii. Kaspersky Internet Security 2009, iii. McAfee Total Protection with Security Center v.9.15, iv. Norton Internet Security 2009 v.16.5.0.135, v. Symantec AntiVirus v.10.1.7.7000, và vi. Trend Micro Internet Security Pro v.17.1.1250

Kết quả thực nghiệm của họ cho thấy mặc dù phát hiện dựa trên hành vi; phần mềm AV không thể phát hiện hiệu quả tất cả các hình thức phần mềm độc hại hiện tại. Tuy nhiên, phát hiện dựa trên hành vi Chua và Balachandran (2018) đã đánh giá Hiệu quả của Obfuscation Android trong việc Tránh Anti-malware. Theo họ, công cụ tự động hóa kiểm soát giao diện lập trình ứng dụng (API) VirusTotal để phân loại các mẫu phần mềm độc hại. Họ tiếp tục sử dụng 57 Công cụ Chống phần mềm độc hại (AMTs) được liệt kê trên VirusTotal, để đánh giá hiệu quả của các kỹ thuật biến đổi được đề xuất của họ, và để làm cho đánh giá có thể mở rộng cho một số lượng lớn mẫu phần mềm độc hại. Họ đã sử dụng phiên bản dòng lệnh của VirusTotal, có thể thực hiện phân tích tĩnh với một mức độ nhất định của cơ sở dữ liệu chữ ký. Công trình của họ chứng minh rằng các tác giả phần mềm độc hại có thể tăng tỷ lệ tránh của phần mềm độc hại bằng cách thực hiện các kỹ thuật obfuscation.

Điểm mới của công trình của họ là việc xác định sự không ổn định trong kết quả phát hiện đối với một số AMTs. Cũng được nhấn mạnh rằng các AMTs không xây dựng khả năng phục hồi/linh hoạt chống lại kỹ thuật được sử dụng để làm mờ phần mềm độc hại, mà chỉ cập nhật cơ sở dữ liệu chữ ký của họ để phục hồi với biến thể cụ thể của phần mềm độc hại. Các xu hướng được nhấn mạnh trong công trình của họ nhấn mạnh sự dễ dàng cuối cùng tránh các công cụ bảo mật chính thống hiện tại đối với một tác giả phần mềm độc hại. Rubenking (2019) liệt kê Avast Free Antivirus, Kaspersky Antivirus, AVG Free Antivirus, Bitdefender Antivirus Free Edition, Check Point ZoneAlarm Free Antivirus+ 2017, Sophos Home Free, Avira Antivirus, Adaware Antivirus Free, Comodo Antivirus 10 và Panda Free Antivirus là 10 sản phẩm antivirus miễn phí tốt nhất.

Trong một đánh giá khác của Zacks (2019), các sản phẩm sau được liệt kê: Norton Security Antivirus, McAfee Free Antivirus, Total AV Free Antivirus, Avira Free Antivirus, Panda Free Antivirus, Intrusta Antivirus, CYLANCE Antivirus, Heimdal Antivirus Free, Webroot SecureAnywhere Free, và Bitdefender Antivirus Free Edition.

Fisher (2019) đề cập rằng Avira Free Security Suite, Bitdefender Antivirus Free, Adaware Antivirus Free, Avast Free Antivirus, Panda Dome, AVG Antivirus Free, COMODO Antivirus Free, FortiClient, Immunet Antivirus, và Kaspersky Free là 10 giải pháp antivirus miễn phí tốt nhất. Tương tự, một đánh giá khác của Wagenseil (2019), các giải pháp antivirus miễn phí nằm trong danh sách 10 đầu là Kaspersky Free Antivirus, Bitdefender Free Antivirus, Avast Free Antivirus, Microsoft Windows Defender, AVG, Avira, Panda, Malwarebytes.

Nhưng, Allen (2019) trình bày 8 sản phẩm antivirus miễn phí tốt nhất là Avast, Bitdefender, AVG, Sophos Home Free, Panda Free Antivirus, ZoneAlarm Free Antivirus, Comodo Antivirus, và Avira Free Antivirus.

Theo Orphanides (2019) Kaspersky Free Antivirus, Microsoft Windows Defender, Bitdefender Free Antivirus, Avira Free Antivirus, Avast Free Antivirus, và AVG Free Antivirus nằm trong danh sách 6 giải pháp antivirus miễn phí tốt nhất. Ngược lại, nghiên cứu này quan tâm đến việc đánh giá hiệu quả của các công cụ tránh antivirus chống lại các giải pháp antivirus, và không kiểm tra các mẫu phần mềm độc hại được thu thập ngẫu nhiên không nhất thiết được làm mờ.

Bảng 1 Tóm tắt Các Công trình Liên quan

Hiển thị Tóm tắt các Tác phẩm Liên quan				
S/N	**Tác giả**	**Nghiên cứu**	**Điểm mạnh**	**Điểm yếu**
1.	Kalogranis (2018)	Tránh Phần mềm AV: Đánh giá Các Công cụ Tránh Antivirus	Sử dụng payload meterpreter tcp ngược phổ biến của Metasploit, và một số tệp mẫu payload tùy chỉnh	Số lượng công cụ tránh nhỏ, và không mã hóa
2.	Themelis (2018)	Công cụ Tránh AV: pyRAT	Sử dụng Metasploit Framework cùng với các tính năng của nó để tự động hóa payload.	Sử dụng payload được định nghĩa trước
3.	Sukwong et al., (2011)	Đánh giá Hiệu quả của Phần mềm AV Thương mại	Sử dụng nhiều kỹ thuật phát hiện	Thử nghiệm được thực hiện trên bộ sưu tập mẫu phần mềm độc hại ngẫu nhiên không nhất thiết được làm mờ
4.	Chua and Balanchandra (2018)	Đánh giá Hiệu quả của Obfuscation Android trong việc Tránh Phần mềm độc hại	Sử dụng số lượng lớn mẫu phần mềm độc hại và 57 Công cụ Chống phần mềm độc hại (AMTs) trên VirusTotal	Phiên bản Dòng lệnh được sử dụng có thể thực hiện phân tích tĩnh với mức độ nhất định của cơ sở dữ liệu chữ ký
5.	Present study (2019)	Đánh giá Hiệu quả của Công cụ Tránh	Sử dụng Metasploit Framework phổ biến	Tạo payload từ framework

		AV chống lại Nền tảng Window Evasion Tools against Window Platform	và mở rộng số lượng phần mềm Tránh	

Sau khi xem xét nhiều nghiên cứu được thực hiện, phát hiện ra rằng, chỉ có một vài công trình đánh giá khả năng hiệu quả của phần mềm tránh miễn phí trên internet đối với các bảo vệ nền tảng window. Vì lý do này, nghiên cứu hiện tại nhằm xác nhận lại nhưng mở rộng công trình của Kalogranis (2018), bằng cách tạo payload sử dụng Metasploit Framework phổ biến. Các công cụ tránh AV được chọn trong nghiên cứu của ông đã được đánh giá lại và các công cụ tránh AV khác có sẵn trong lưu thông công khai không được bao gồm trong nghiên cứu cũng được xem xét.

4. Phương pháp

Lựa chọn Sản phẩm Antivirus Miễn phí

Để lựa chọn sản phẩm antivirus miễn phí, dựa trên các nguồn được xem xét, chúng tôi đã trao điểm cho mỗi antivirus xuất hiện trong một đánh giá là 1 điểm. Do đó, các sản phẩm antivirus có điểm cao nhất đã được chọn cho nghiên cứu này. Như được mô tả trong Bảng 2.

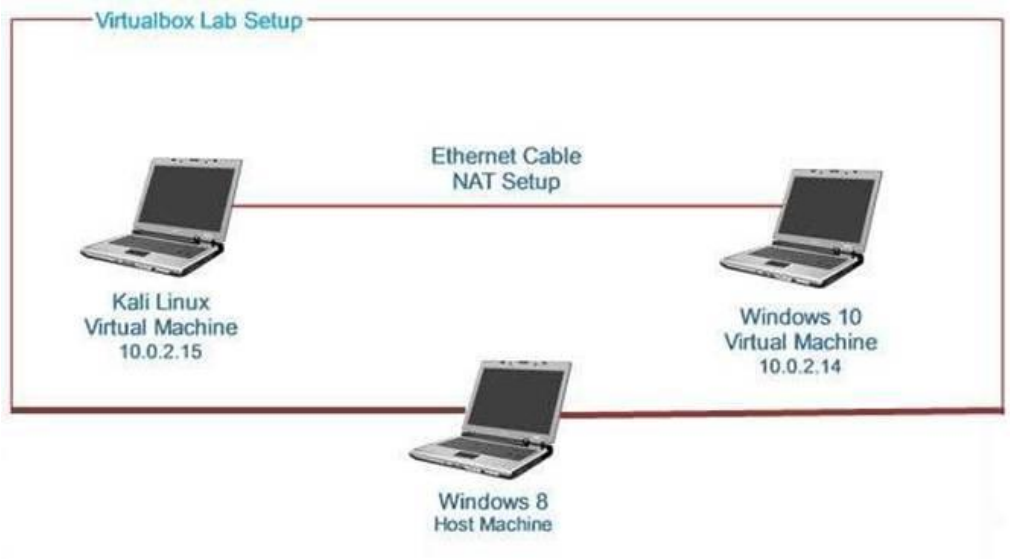
Bảng 2: Lựa chọn Sản phẩm AV

Antivirus Score	J.N. Rubenking (2019)	T. Fisher (2019)	P. Wagensei (2019)	J. Allen (2019)	K. G. Orphanides (2019)	**AV rating Scores**
Avast AV	1	1	1	1	1	**5**
Kaspersky AV	1	1	1	0	1	**4**
AVG Free AV	1	1	1	1	1	**5**
Bitdefender AV Free	1	1	1	1	1	**5**
Check Point	1	0	0	0	0	1
ZoneAlarm Free AV	0	0	0	1	0	1
Sophos Home Free	1	0	0	0	0	1

Avira Antivirus	1	1	1	1	1	**5**
Adaware AVFree	1	1	0	0	0	2
Comodo Antivirus 10.3	1	1	0	1	0	3
Panda Free Antivirus 4	1	1	1	0	1	**4**
Total AV Free	0	0	0	0	0	0
Norton Free AV	0	0	0	0	0	0
McAfee Free Antivirus	0	0	0	0	0	0
Intrusta Antivirus	0	0	0	0	0	0
CYLANCE Antivirus	0	0	0	0	0	0
Heimdal Antivirus Free	0	0	0	0	0	0
Webroot Secure A.Free	0	0	0	0	0	0
FortiClient	0	1	0	0	0	1
Immunet Antivirus	0	1	0	0	0	1
Windows Defender	0	1	0	0	1	2

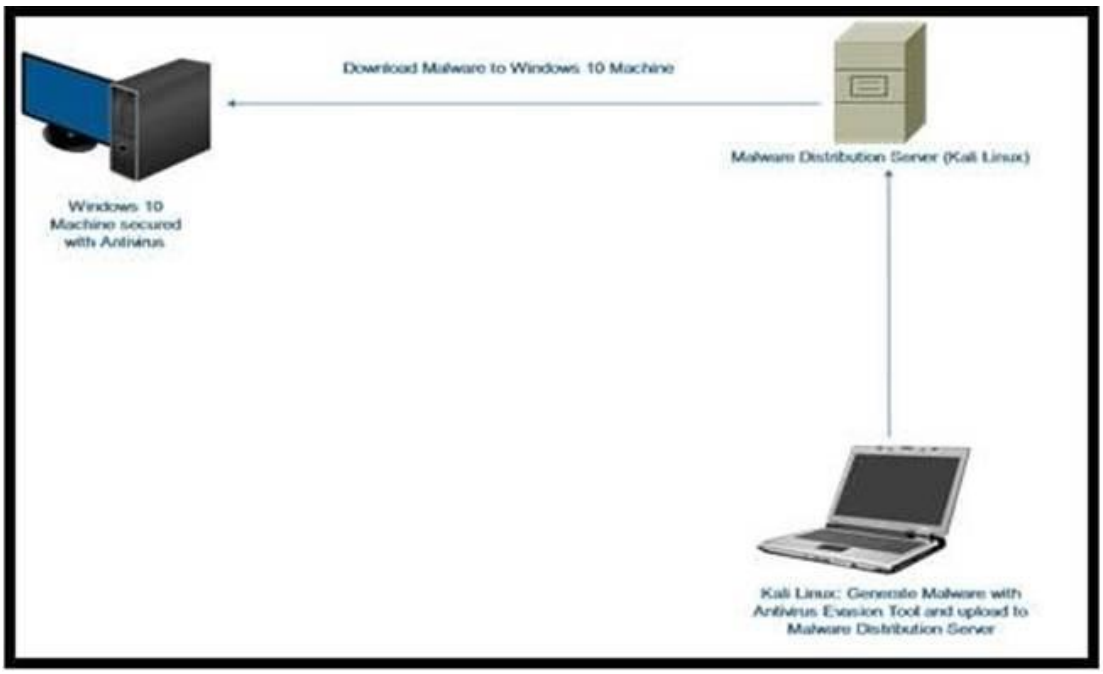
Quy trình thực nghiệm

Thực nghiệm được thực hiện trong một phòng thí nghiệm, thiết lập với VM VirtualBox trên máy chủ Windows 8 64-bit với bộ xử lý Intel Core i4, 10GB RAM và 500GB HDD. Hai máy ảo, máy tạo phần mềm độc hại "Kali Linux" và máy mục tiêu "Windows 10" được kết nối mạng và sử dụng qua cáp Ethernet, NAT (Network Address Translation) như được thấy trong Hình 1.



Hình 1: Môi trường Phòng thí nghiệm Ảo

Tất cả các công cụ tránh đã được cài đặt trên máy Kali Linux để tạo mẫu phần mềm độc hại và triển khai đến các máy mục tiêu (Windows 10) qua máy chủ phân phối phần mềm độc hại để các máy mục tiêu tải xuống và chạy để thực thi. Như được đơn giản hóa thêm trong Hình 2.



Hình 2: Kiến trúc Hệ thống Phòng thí nghiệm

Các giải pháp antivirus cũng được cài đặt từng cái một, kiểm tra với phần mềm độc hại được tạo từ một trong các công cụ tránh. Sau đó, các thử nghiệm tiếp tục cho đến khi tất cả các sản phẩm phần mềm AV được chọn đã được kiểm tra. Trong quá trình đánh giá, nếu phần mềm antivirus phát hiện phần mềm độc hại, điểm 1 được trao cho antivirus; nếu không, điểm 0 được trao. Từ đó, công cụ tránh được trao điểm 1 nếu nó có thể vượt qua antivirus và điểm 0 nếu không. Cuối cùng, phần mềm antivirus có điểm phát hiện cao nhất được trao hiệu quả

nhất. Ngoài ra, công cụ tránh có điểm cao nhất được trao công cụ tránh antivirus tốt nhất trong nghiên cứu này. Sau đó, kết quả thử nghiệm được ghi lại và so sánh với công trình gần đây của Kalogranis (2018).

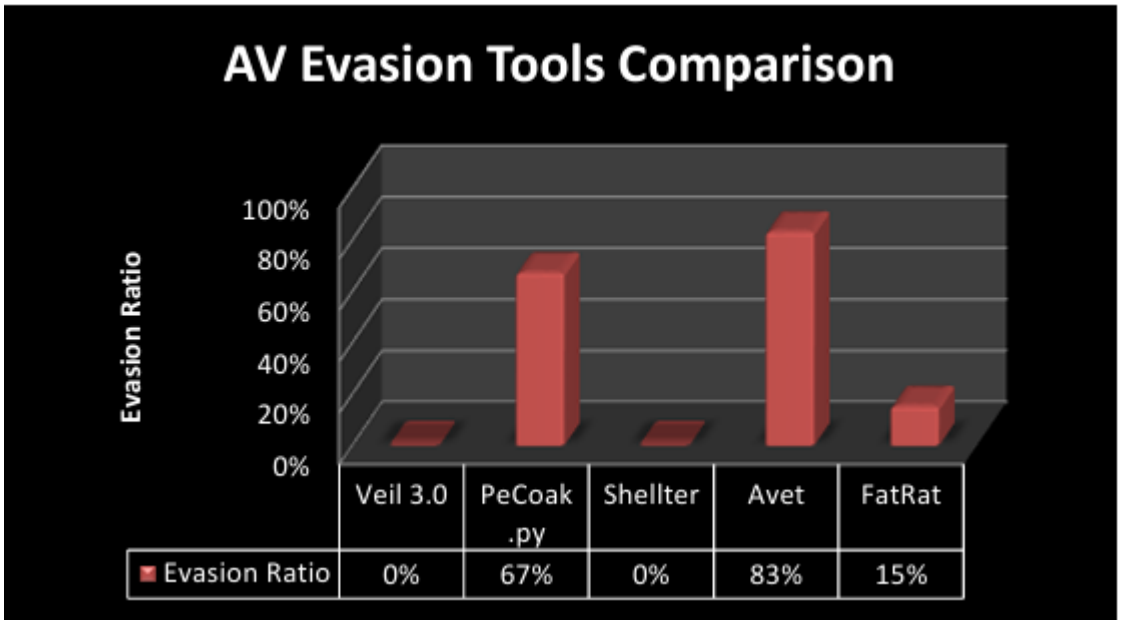
5. Kết quả và thảo luận

Metasploit window reverses TCP metepreter phổ biến đã được sử dụng trong bài báo này, để mã hóa payload. Theo Beer và Hornat (2006), Metasploit được thiết kế và dễ sử dụng, cho mục đích kiểm tra thâm nhập. Cũng được đề cập rằng; Các Bảng được liệt kê dưới đây hiển thị điểm số được ghi lại cho mỗi Metasploit framework có thể được sử dụng để khai thác bất kỳ mục tiêu nào trong phần mềm antivirus và công cụ tránh AV được sử dụng trong nghiên cứu này. hệ thống hoặc cơ sở hạ tầng mạng.

Bảng 8: Tóm tắt kết quả thử nghiệm của các Công cụ Tránh Antivirus

S/N	Công cụ Tránh AV	Avira	Bitdefender	Avast	Antivirus Free Kaspersky	AVG	Panda	Tổng điểm Công cụ Tránh
1.	Veil 3.0	0						**0**
2.	PeCloak.py	1	0	1	0	1	1	**4**
3.	Shellter	0						**0**
4.	Avet	1	1	1	0	1	1	**5**
5.	Fat Rat	0	1	0	0	0	0	**1**

Các tỷ lệ tránh giữa các công cụ tránh antivirus được so sánh ở đây. Trong nghiên cứu này, các tỷ lệ tránh (AVs bị tránh/Số lượng AV Được chọn Tổng cộng) dao động từ 0% đến 83%. Tránh PeCoak.py được quan sát với tỷ lệ tránh 67%, Avet báo cáo tỷ lệ tránh cao nhất là 83%, trong khi Fatrat với 15%, thấp nhất 0% cho cả Veil và Shellter, như được mô tả trong Hình 3.

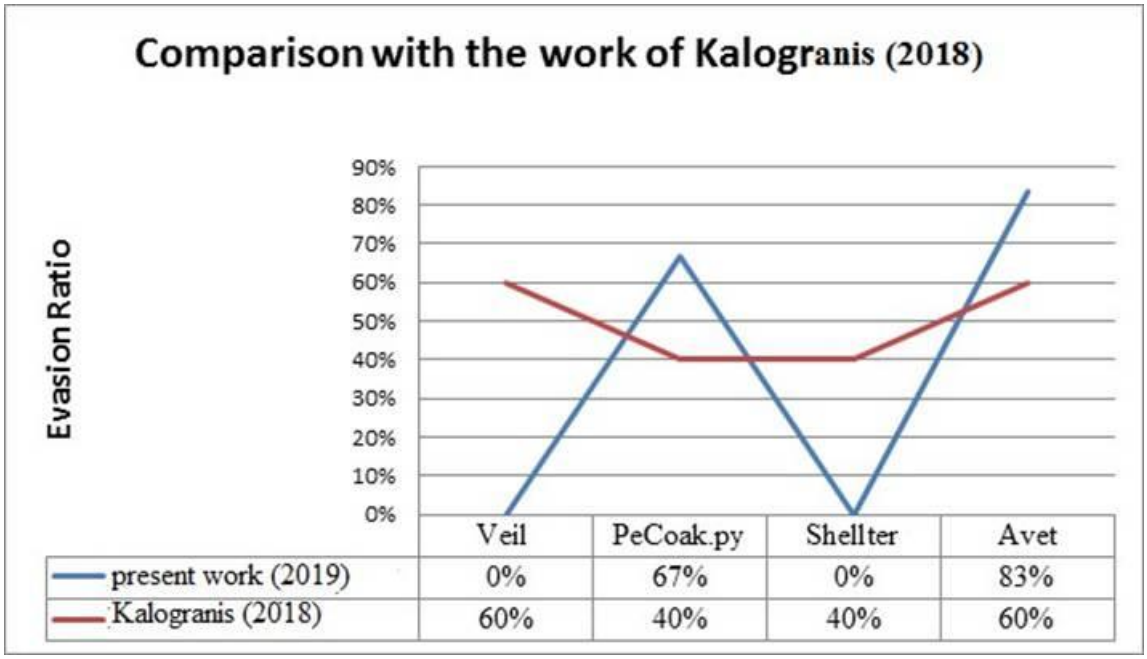


Hình 3: So sánh Công cụ Tránh AV

Kết quả trong Bảng 8 tiết lộ rằng công cụ tránh Avet báo cáo hiệu suất công cụ tránh tốt nhất, kỹ thuật được sử dụng trong Avet đã tránh 5 trong số 6 bộ Anti-virus. Avet bao gồm hai công cụ, avet.exe và kỹ thuật tránh AV để tránh sandboxing và mô phỏng. Avet.exe biên dịch tệp nhị phân được cấu hình trước và có khả năng tải shellcode được mã hóa ASCII từ tệp văn bản hoặc từ máy chủ web. Trong khi công cụ tránh peCloak.py trở thành thứ hai để vượt qua 4 trong số 6 AV. Công cụ tránh Fat rat chỉ có thể tránh 1 trong số 6 AV. Do đó, không có AV nào có thể bị vượt qua bởi shelter và công cụ tránh Veil 3.0. Đối với thất bại của Veil 3.0, cần chạy lại script để cài đặt bất kỳ gói bổ sung nào và cập nhật các tệp cấu hình chung. Và trong trường hợp Shellter, hiện chỉ có ứng dụng 32-bit, tại thời điểm nghiên cứu này, trong khi hệ thống phòng thí nghiệm sử dụng ứng dụng window 64-bit. Sự khác biệt này cũng có thể mang lại kết quả không hiệu quả cho công cụ tránh Shellter. Shellter có khả năng lấy bất kỳ ứng dụng Window 32-bit nào và nhúng shellcode, hoặc bằng payload tùy chỉnh hoặc một cái có sẵn từ. Metasploit framework như được sử dụng trong nghiên cứu này, theo cách rất thường không thể phát hiện bởi phần mềm AV. Nếu ứng dụng 32-bit được sử dụng, bạn có thể tạo gần như vô số chữ ký khiến phần mềm AV gần như không thể phát hiện.

Một số kết quả thu được trong nghiên cứu này khác với phát hiện của Kalogranis (2018) có tỷ lệ tránh (AVs bị tránh/Số lượng AV được chọn Tổng cộng) từ 40% đến 60%, trong khi 0% đến 83% được chú ý trong nghiên cứu hiện tại này.

Trong nghiên cứu này, công cụ tránh Veil 3.0 không thể vượt qua tất cả các bảo vệ phần mềm antivirus được sử dụng, trong khi trong công trình của Kalogranis là 60%, PeCloak.py đạt tỷ lệ tránh 67%, trong khi 40% trong công trình của Kalogranis (2018). Shellter cũng có tỷ lệ tránh yếu nhất, trong nghiên cứu này, trong khi shellter báo cáo tỷ lệ tránh 40% trong công trình của Kalogranis (2018). Trong cả hai công trình, Avet duy trì tỷ lệ tránh cao trong khi 60% trong nghiên cứu của Kalogranis (2018) như được hiển thị trong Hình 4.



\

Hình 4: So sánh Kalogranis (2018) và Nghiên cứu Hiện tại

Kết quả của hai nghiên cứu so sánh trong Hình 4 khác nhau; điều này là vì các nhà thiết kế phần mềm chống phần mềm độc hại cải thiện nỗ lực của họ, nâng cao độ chính xác phát hiện bằng cách cập nhật các tệp chữ ký của sản phẩm bảo vệ phần mềm, trong khi một số nhà thiết kế nâng cấp từ kỹ thuật phát hiện dựa trên chữ ký truyền thống sang kỹ thuật phát hiện dựa trên hành vi. Ngoài ra, tệp mẫu độc hại, (Portable Executable) được tạo bởi các Công cụ Tránh được sử dụng trong nghiên cứu này là payload được định nghĩa trước. Chúng được tạo bằng cách sử dụng các framework phổ biến và không có payload tùy chỉnh nào được tiêm. Trong khi trong nghiên cứu của Kalogranis (2018), hầu hết các nỗ lực tốt nhất thu được từ các Công cụ Tránh là với payload tùy chỉnh. Và công trình của Chua và Balachandran (2018) chỉ xem xét obfuscation như một kỹ thuật tránh và không có công cụ nào được xác định. Nghiên cứu cũng khác với nghiên cứu này vì các nhà nghiên cứu nhắm đến nền tảng window, không phải android.

6. Kết luận

Kết luận, kết quả thu được trong nghiên cứu này đã chứng minh Avet và PeCloak.py AV công cụ tránh là tốt nhất đã vượt qua hầu hết các antivirus được chọn với 83% và 67% tương ứng. Mặt khác, Kaspersky và Bitdefender antivirus xuất hiện là phần mềm bảo vệ hiệu suất tốt nhất để phát hiện các thủ đoạn tránh phần mềm độc hại. Ngoài ra, dựa trên so sánh được thực hiện giữa nghiên cứu hiện tại này và Kalogranis (2018), cho thấy tốt hơn là viết payload tùy chỉnh và giữ chúng đơn giản để tránh phát hiện AV thay vì tạo payload bằng cách sử dụng các framework phổ biến. Tuy nhiên, kết quả thu thập có thể vẫn thay đổi khi các sản phẩm AV liên tục cập nhật các tệp chữ ký sản phẩm AV.

Cuối cùng, người dùng hệ thống máy tính được khuyến nghị sử dụng bảo vệ phần mềm antivirus được chỉ định trong nghiên cứu này, cho bảo vệ hệ thống tốt nhất. Ngoài ra, Công cụ Tránh AV Avet và PecCloak.py được khuyến nghị cho các hoạt động kiểm tra thâm nhập.