Bài: 3.3 Quét mạng - Vẽ sơ đồ mạng

Xem bài học trên website để ủng hộ Kteam: 3.3 Quét mạng - Vẽ sơ đồ mạng

Mọi vấn đề về lỗi website làm ảnh hưởng đến bạn hoặc thắc mắc, mong muốn khóa học mới, nhằm hỗ trợ cải thiện Website. Các bạn vui lòng phản hồi đến Fanpage How Kteam nhé!

Vẽ sơ đồ mạng

Để truy cập được vào một mạng máy tính, việc cần thiết là hiểu sâu sắc về cấu trúc của mạng và thu thập thông tin về mạng. Những thông tin có giá trị như **vùng bảo mật** (Security Zones), thiết bị bảo mật, số host,.v.v của mạng giúp tin tặc hiểu được sơ đồ của mạng. Một khi sơ đồ mạng được thiết kế, sơ đồ đó sẽ xác định những lối đi đến mục tiêu phù hợp bên trong một mạng.

Sơ đồ mạng cho thấy môi trường mạng và cung cấp một bức tranh thậm chí hoàn hảo hơn về mạng máy tính đó. **Network Mappers** là những công cụ vẽ bản đồ mạng, sử dụng công nghệ scan và những công cụ khác để vẽ một bức tranh về mang. Điều quan trọng cần quan tâm đó là, những công cụ này làm phát sinh những traffic có thể tiết lộ sự hiện diện của tin tặc hoặc các pentester trong mạng.

Công cụ khám phá mạng

OpManager là một công cụ điều hành mạng tiên tiến giúp điều khiển các lỗi, hỗ trợ các đường link WAN, Router, Switch, VoIP và các server. Nó cũng có thể thực hiện việc quản trị hiệu quả làm việc. **Network View** là một công cụ khám phá mạng tiên tiến. Nó có thể thực hiện việc khám phá các route, các điểm TCP/IP sử dụng DNS, các port, và các giao thức mạng khác. Một vài công cụ phổ biến là:

1. Network Topology Mapper
2. OpManager
3. Network View
4. LANState Pro

Vẽ sơ đồ mạng

Solar Wind Network Topology Mapper có thể khám phá mạng và tạo một sơ đồ bao quát mạng. Phần mềm cũng cung cấp nhiều chức năng cộng thêm như chỉnh sửa nodes bằng tay, xuất ra sơ đồ đến Visio, khám phá những mạng nhiều tầng,v.v. Mapper topology có thể hiển thị tên Node, địa chỉ IP, Hostname, tên hệ thống, loại máy móc, các Vendor, định vị hệ thống và các thông tin khác.

Lab 3-4 Tạo Network Topology Map với công cụ

Tạo Network Topology Map

Với công cụ **SolarWind Network Topology mapper**, hãy bắt đầu scan mạng bằng cách click chuột vào nút **New Network Scan**

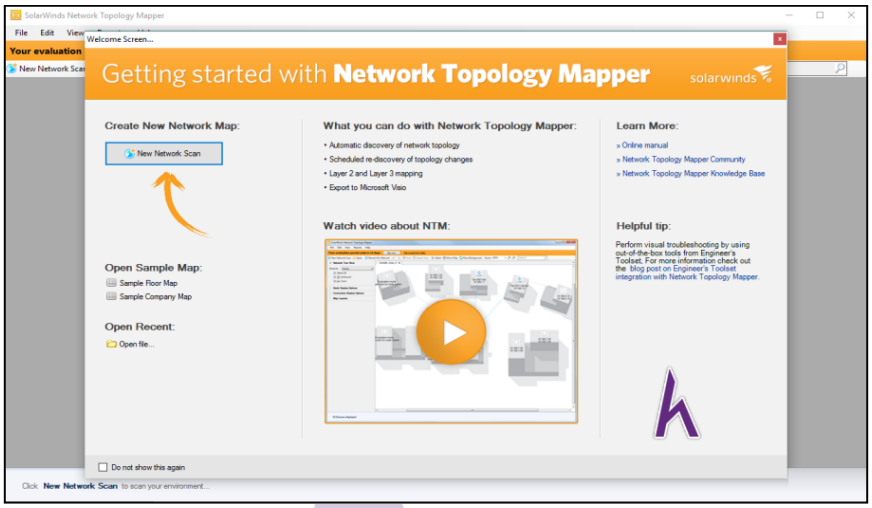


Figure 3-42 Network Topology Mapper Tool

Thêm thông tin mạng, định hình cài đặt khám phá, giấy tờ ủy nhiệm nếu cần

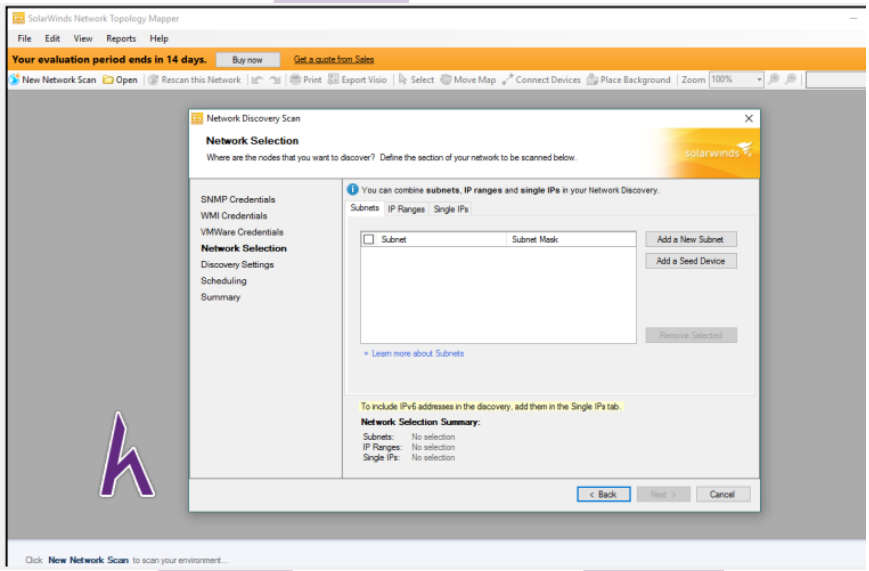


Figure 3-43 Configuring Scan

Khi đã hoàn thành các thiết đặt, bắt đầu **Scan**

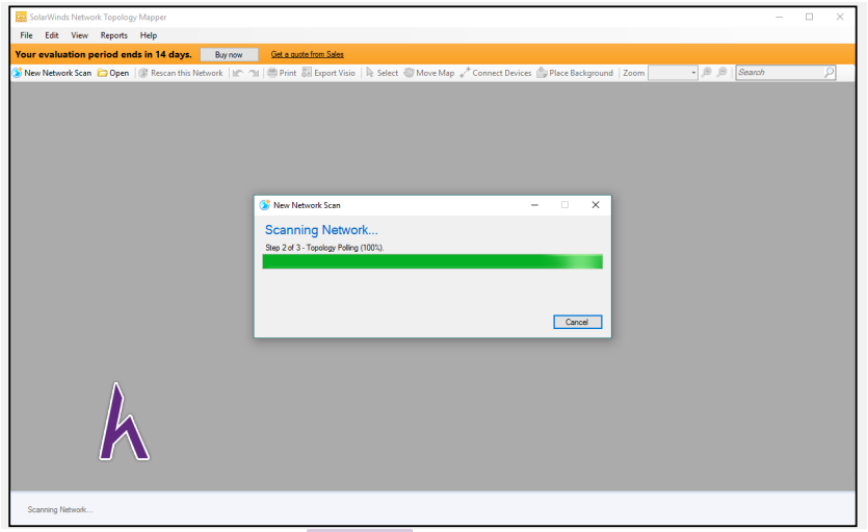
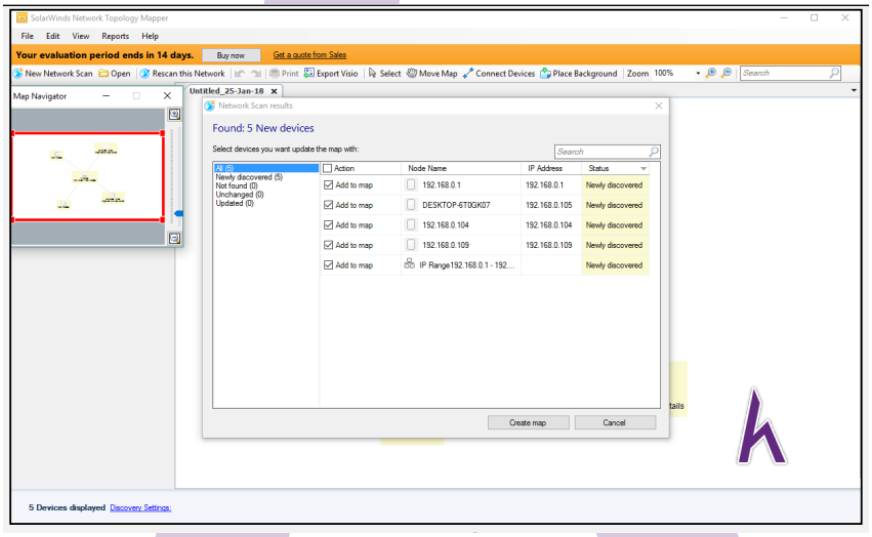


Figure 3-44 Scanning Network

Sau khi hoàn thành quá trình quét,một danh sách những thiết bị tìm được sẽ được thêm vào sơ đồ. Chọn tất cả hoặc những thiết bị cần thiết để thêm vào topology.



Giờ bạn có thể thêm các node bằng tay, xuất đến Vision và sử dụng những chức năng khác của công cụ

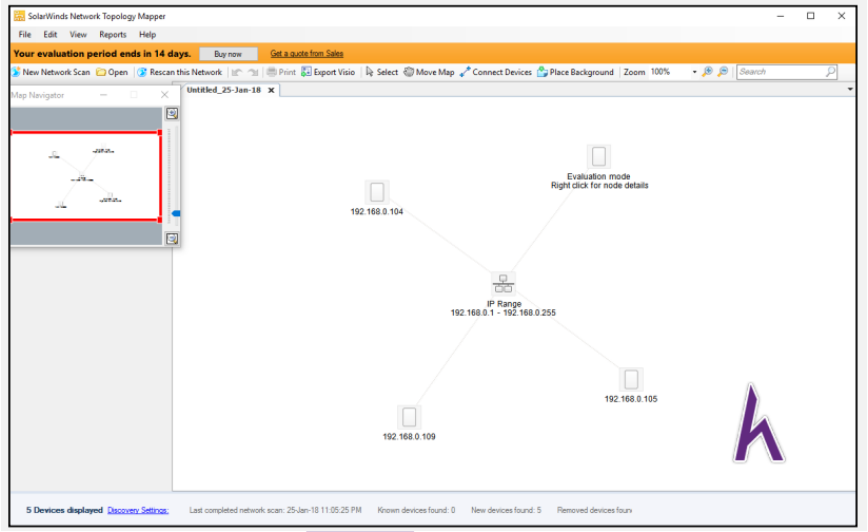


Figure 3-46 Topology

Chuẩn bị Proxies

Proxy là hệ thống nằm giữa tin tặc và mục tiêu. **Hệ thống proxy** đóng một vai trò quan trọng trong mạng. Hệ thống proxy cơ bản được sử dụng bởi các máy scan để làm ẩn đi đặc điểm của nó để theo dõi lại mục tiêu.

Proxies Servers

Proxy Server giấu đi lưu lượng truy cập web nhằm cung cấp chế độ nặc danh. Khi người dùng gửi đi yêu cầu cho bất cứ tài nguyên nào đến những server công cộng có sẵn, proxy server sẽ hoạt động như một cầu nối rung gian cho những yêu cầu đó. Yêu cầu của người dùng được đẩy tới proxy server đầu tiên.

Proxy Server sẽ trao đổi những yêu cầu đó như những trang web, file download, kết nối đến một server khác. Dạng phổ biến nhất của proxy server là ở dưới dạng web proxy server. Những web proxy server này được sử dụng để cung cấp quyền truy cập cho mạng toàn cầu bằng cách vượt qua tường địa chỉ IP.

- Khi sử dụng Proxy Server, tóm tắt lại, có thể tổng kết lại như sau:
- Ẩn đi nguồn địa chỉ IP cho việc vượt qua tường địa chỉ IP
- Mạo nhận
- Truy cập tintranet từ xa
- Điều hướng toàn bộ yêu cầu đến proxy server để ẩn đi nhận dạng
- Proxy Chaining để tránh bị phát hiện

Proxy Chaining

Proxy Chaining cơ bản là công nghệ sử dụng nhiều proxy server. Cùng với proxy servers, một proxy server đẩy lưu lượng người dùng tới proxy server tiếp theo. Quy trình này không được đề xuất cho môi trường sản xuất, hoặc giải pháp lâu dài, tuy nhiên, công nghệ này thúc đẩy proxy đang tồn tại của bạn

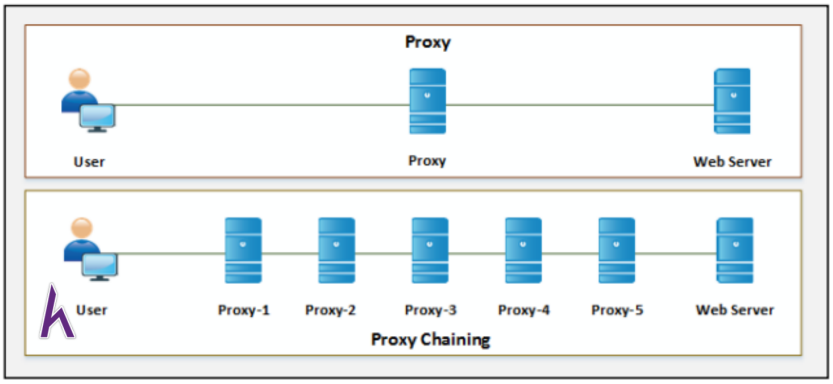


Figure 3-48 Proxy Chaining

Công cụ Proxy

Có những **công cụ proxy** khả dụng cũng như bạn có thể tìm kiếm các proxy server và định dạng chúng bằng tay ngay trên trình duyệt web. Những công cụ này bao gồm:

1. Proxy swicher
2. Proxy Workbench
3. TOR
4. CyberGhost

Proxy Switcher

Công cụ **Proxy Switcher** scan những proxy server khả dụng. Bạn có thể bật bất cứ proxy server nào để ẩn địa chỉ IP của bạn. Những mô tả dưới đây cho thấy quá trình tìm kiếm của Proxy với công cụ **Proxy Switcher**

Công cụ Proxy cho điện thoại

Có nhiều ứng dụng proxy khả dụng trên google play và App store cho các thiết bị di động:

Application	Download URL
Proxy Droid	https://play.google.com
Net Shade	https://itunes.apple.com

Giới thiệu Anonymizers

Anonymizer là một công cụ hoàn toàn ẩn đi hoặc loại bỏ những thông tin nhận dạng có liên quan để tạo ra những hoạt động không thể bị lần theo dấu vết. Mục đích cơ bản khi sử dụng anonymizer là:

- Giảm thiểu nguy hiểm
- Nhận dạng ngăn cản đánh cắp
- Bỏ qua giới hạn và kiểm duyệt
- Hoạt động không để lại dấu vết trên internet

Công cụ phá vỡ tầng kiểm duyệt

Tail

Tail (The Amnesic Incognito Live System) là một công cụ phá vỡ kiểm duyệt dựa trên **Debian GNU/Linux**. Cơ bản đó là một hệ điều hành hoạt động có thể chạy trên mọi máy tính từ USB hoặc DVD. Hệ điều hành này được thiết kế đặc biệt để giúp bạn sử dụng internet ẩn danh mà không để lại dấu vết. Tail bảo mật thông tin riêng tư và giấu tên.

Các Anonymizers cho điện thoại

- Orbot
- Psiphon
- Open door

Địa chỉ IP lừa đảo

Lừa đảo địa chỉ IP là một công nghệ sử dụng để lấy quyền truy cập trái phép vào máy móc bằng cách dùng IP lừa đảo. Một tin tặc mạo danh trái phép bất cứ máy móc nào bằng cách gửi đi gói IP với địa chỉ IP lừa đảo.

Quy trình đánh lừa bao gồm việc điều chỉnh header với một nguồn địa chỉ IP giả, tổng kiểm tra và sắp đặt giá trị. **Mạng chuyển mạch** (Packet-switched networking) khiến cho các gói tin đến điểm đích theo thứ tự khác nhau. Khi những gói tin sai thứ tự đã đến đích, các gói tin này sẽ được tập hợp lại để giải nén tin nhắn.

IP giả có thể bị phát hiện bởi nhiều công nghệ bao gồm công nghệ thăm dò **Direct TTL** và qua **IP Identification Number**. Trong quá trình gửi đi thăm dò TTL trực tiếp, các gói tin được gửi tới những host bị nghi ngờ là gửi gói tin giả mạo và phản hồi sẽ được quan sát. Bằng cách so sánh giá trị TTL từ phản hồi của host khả nghi, IP giả có thể bị phát hiện. Đó sẽ là gói tin giả mạo nếu giá trị TTL không giống với giá trị trong gói tin.

Tuy nhiên, giá trị TTL có thể dao động ngay cả trong lưu lượng bình thường và công nghệ này sẽ nhận dạng lừa đảo nếu tin tặc đang ở một subnet khác

Tương tự, những thăm dò thêm vào được gửi đi để xác thực IPID của host. Nếu giá trị IPID không gần giống, lưu lượng đáng nghi là lừa đảo. Công nghệ này có thể được sử dụng trong trường hợp tin tặc đang ở trong subnet