

Bài: 4.2 Điều tra - Điều tra SNMP, LDAP, NTP, SMTP & biện pháp đối phó điều tra

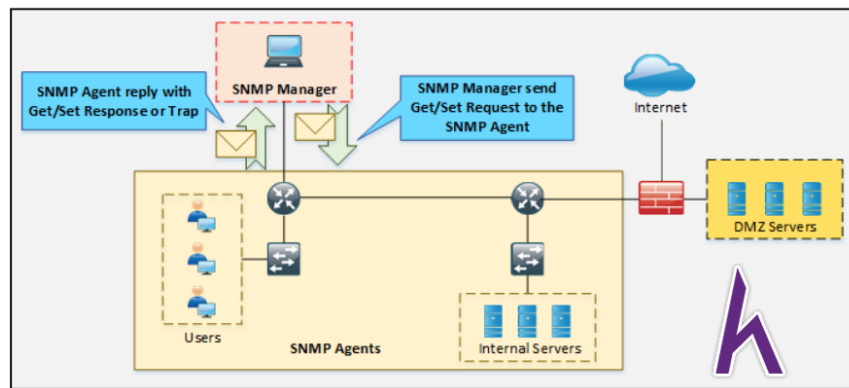
Xem bài học trên website để ủng hộ Kteam: [4.2 Điều tra - Điều tra SNMP, LDAP, NTP, SMTP & biện pháp đối phó điều tra](#)

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!

Điều tra SNMP (SNMP Enumeration)

SNMP Enumeration

Giao thức quản lý mạng đơn giản (SNMP) là một kỹ thuật điều tra sử dụng giao thức quản lý mạng được sử dụng rộng rãi nhất SNMP. Trong Điều tra SNMP, tài khoản người dùng và thông tin thiết bị được nhắm mục tiêu bằng SNMP. SNMP yêu cầu chuỗi cộng đồng để xác thực trạm quản lý.



Chuỗi cộng đồng này ở các dạng khác trong các phiên bản khác nhau của SNMP. Sử dụng chuỗi cộng đồng mặc định, bằng cách đoán chuỗi cộng đồng, kẻ tấn công trích xuất thông tin như máy chủ, thiết bị, chia sẻ, thông tin mạng và nhiều hơn thế nữa bởi được truy cập trái phép.

Chuỗi cộng đồng	Mô tả
SNMP Read-only community string	Cho phép thiết bị từ xa truy xuất thông tin "chỉ đọc" từ thiết bị.
SNMP Read-Write community string	Được sử dụng trong các yêu cầu thông tin từ thiết bị và để sửa đổi cài đặt trên thiết bị đó.
SNMP Trap community string	Gửi SNMP Traps tới InterMapper.

Giao thức quản lý mạng đơn giản (Simple Network Management Protocol)

Trong môi trường sản xuất, nơi hàng nghìn thiết bị mạng như bộ định tuyến, thiết bị chuyển mạch, máy chủ và thiết bị đầu cuối được triển khai, **Network Operation Center** (NOC) phải đóng một vai trò rất quan trọng. Hầu hết mọi nhà cung cấp đều hỗ trợ **giao thức quản lý mạng đơn giản** (SNMP). Ban đầu, triển khai SNMP yêu cầu trạm quản lý. Trạm quản lý thu thập thông tin về các khía cạnh khác nhau của thiết bị mạng. Điều thứ hai là cấu hình và hỗ trợ phần mềm bằng chính các thiết bị mạng. Cấu hình như loại mã hóa và được chia nhỏ chạy trên phần mềm của trạm quản lý phải khớp với cài đặt SNMP trên thiết bị mạng.

Về mặt kỹ thuật, ba thành phần có liên quan đến việc triển khai SNMP trong một mạng:

Trình quản lý SNMP (SNMP Manager)

Một ứng dụng phần mềm chạy trên trạm quản lý để hiển thị thông tin được thu thập từ các thiết bị mạng một cách tinh tế và có thể biểu diễn. Phần mềm SNMP thường được sử dụng là PRTG, Solarwinds, OPManger, v.v.

Đại lý SNMP (SNMP Agent)

Phần mềm đang chạy trên các nút mạng có các thành phần khác nhau cần phải được theo dõi. Ví dụ bao gồm sử dụng CPU / RAM, trạng thái giao diện, v.v. Số cổng UDP 161 được sử dụng để liên lạc giữa đại lý SNMP và trình quản lý SNMP.

Cơ sở thông tin quản lý (Management Information Base):

MIB là viết tắt của **Management Information Base** và là một tập hợp các thông tin được tổ chức theo cấp bậc trong một cơ sở dữ liệu ảo. Chúng được truy cập bằng giao thức như SNMP.

Có hai loại MIB:

Các loại MIB	Mô tả
Scaler	Nó định nghĩa một cá thể đối tượng đơn lẻ.
Tabular	Nó định nghĩa nhiều cá thể đối tượng liên quan.

Các **đối tượng vô hướng** xác định một cá thể đối tượng đơn lẻ trong khi các **đối tượng dạng bảng** xác định nhiều cá thể đối tượng liên quan được nhóm trong các bảng MIB.

MIB là tập hợp các định nghĩa, xác định các thuộc tính của đối tượng được quản lý trong thiết bị được quản lý. Bộ sưu tập thông tin này như mô tả các đối tượng mạng được tổ chức và quản lý theo thứ bậc trong MIB và sử dụng SNMP được giải quyết thông qua bộ nhận dạng đối tượng (OID).

Các định danh đối tượng (OID) này bao gồm các đối tượng MIB như chuỗi, địa chỉ, số lượt truy cập, cấp truy cập và thông tin khác. MIB ví dụ: Các đối tượng điển hình để theo dõi trên máy in là các trạng thái hộp mực khác nhau và có thể là số lượng tệp đã in và trên chuyển đổi, các đối tượng tiêu biểu quan tâm là lưu lượng đến và đi cũng như tốc độ mất gói tin hoặc số gói được gửi đến địa chỉ quảng bá.

Các tính năng của các biến thể SNMP có sẵn là:

Phiên bản	Mô tả
V1	Không hỗ trợ mã hóa và chia nhỏ. Chuỗi cộng đồng văn bản thuần túy là được sử dụng để xác thực.
V2c	Không hỗ trợ mã hóa và chia nhỏ. Một số chức năng tuyệt vời như khả năng nhận dữ liệu hàng loạt từ các đại lý được triển khai trong phiên bản 2c.
V3	Hỗ trợ cả mã hóa (DES) và chia nhỏ (MD5 hoặc SHA). Việc triển khai phiên bản 3 có ba mô hình. NoAuthNoPriv nghĩa là không sử dụng mã hóa và chia nhỏ. AuthNoPriv chỉ sử dụng chia nhỏ dựa trên MD5 hoặc SHA sẽ được sử dụng. AuthPriv có nghĩa là cả mã hóa và chia nhỏ sẽ được sử dụng cho lưu lượng SNMP.

Công cụ Điều tra SNMP (SNMP Enumeration Tool)

OpUtils

OpUtils là một công cụ theo dõi mạng và khắc phục sự cố cho các kỹ sư mạng. **OpUtils** được cung cấp bởi Manage Engines, hỗ trợ số lượng công cụ cho **Switch Port & IP Address Management**. Nó giúp các kỹ sư mạng quản lý thiết bị và không gian địa chỉ IP một cách dễ dàng. Nó thực hiện giám sát mạng, phát hiện xâm nhập thiết bị lừa đảo, giám sát sử dụng băng thông và hơn thế nữa.

Tải web: <https://www.manageengine.com/>

Bộ công cụ của SolarWinds Engineer (SolarWinds Engineer's Toolset)

Bộ công cụ của kỹ sư SolarWinds là công cụ quản trị mạng cung cấp hàng trăm công cụ mạng để phát hiện và khắc phục sự cố cũng như chẩn đoán mạng.

Tải web : <https://www.solarwinds.com/>

Các tính năng chính:

- Phát hiện mạng tự động
- Theo dõi và cảnh báo trong thời gian thực
- Khả năng chẩn đoán công hiệu
- Cải thiện an ninh mạng
- Cấu hình và quản trị Registry
- Giám sát địa chỉ IP và phạm vi DHCP

Điều tra LDAP (LDAP Enumeration)

Giao thức truy cập thư mục hạng nhẹ (LDAP) (Lightweight Directory Access Protocol (LDAP))

Giao thức truy cập thư mục hạng nhẹ LDAP là một giao thức Internet chuẩn mở. LDAP là để truy cập và duy trì các dịch vụ thông tin thư mục phân tán trong một cấu trúc phân cấp và hợp lý. Dịch vụ thư mục đóng một vai trò quan trọng bằng cách cho phép chia sẻ thông tin như người dùng, hệ thống, mạng, dịch vụ, v.v. trên toàn mạng.

LDAP cung cấp một nơi trung tâm để lưu trữ tên người dùng và mật khẩu. Các ứng dụng và dịch vụ kết nối với máy chủ LDAP để xác thực người dùng. Máy khách khởi tạo một phiên LDAP bằng cách gửi một yêu cầu hoạt động tới **Directory System Agent (DSA)** bằng cách sử dụng cổng TCP 389. Giao tiếp giữa Client và Server sử dụng **Basic Encoding Rules (BER)**.

Các dịch vụ thư mục sử dụng LDAP bao gồm:

- Active Directory
- Open Directory
- Oracle iPlanet
- Novell eDirectory
- OpenLDAP

Công cụ Điều tra LDAP (LDAP Enumeration Tool):

Công cụ Điều tra LDAP có thể được sử dụng để Điều tra các hệ thống và dịch vụ hỗ trợ LDAP bao gồm:

Công cụ Điều tra LDAP	Trang web
JXplorer	www.jxplorer.org
LDAP Admin Tool	www.ldapsoft.com
LDAP Account Manager	www.ldap-account-manager.org
Active Directory Explorer	technet.microsoft.com
LDAP Administration Tool	sourceforge.net
LDAP Search	securityexploded.com
Active Directory Domain Services Management Pack	www.microsoft.com
LDAP Browser/Editor	www.novell.com



Điều tra NTP (NTP Enumeration)

Giao thức thời gian mạng (NTP) (Network Time Protocol (NTP))

NTP là **giao thức thời gian mạng** được sử dụng trong mạng để đồng bộ hóa đồng hồ trên máy chủ và thiết bị mạng. NTP là một giao thức quan trọng, như dịch vụ thư mục, thiết bị mạng và máy chủ dựa trên cài đặt đồng hồ cho mục đích đăng nhập và ghi nhật ký để lưu giữ hồ sơ các sự kiện.

NTP giúp trong các sự kiện tương quan bởi các bản ghi hệ thống thời gian được nhận bởi các máy chủ Syslog. NTP sử dụng số cổng UDP 123 và toàn bộ giao tiếp của nó dựa trên thời gian phối hợp quốc tế (UTC).

NTP sử dụng thuật ngữ được gọi là tầng để mô tả khoảng cách giữa máy chủ NTP và thiết bị. Nó giống như số TTL làm giảm mỗi hop một gói đi qua. Stratum giá trị, bắt đầu từ một, tăng theo từng hop. Ví dụ, nếu chúng ta thấy số tầng 10 trên bộ định tuyến cục bộ, nó có nghĩa là máy chủ NTP cách chín bước nhảy.

Bảo vệ NTP cũng là một khía cạnh quan trọng vì kẻ tấn công có thể thay đổi thời gian ở vị trí đầu tiên để đánh lừa các nhóm pháp y điều tra và tương quan các sự kiện để tìm nguyên nhân gốc rễ của cuộc tấn công.

Xác thực NTP (NTP Authentication)

NTP phiên bản 3 (NTPv3), và các phiên bản sau này hỗ trợ kỹ thuật xác thực mật mã giữa các đồng nghiệp **NTP**. Xác thực này có thể được sử dụng để giảm thiểu một cuộc tấn công.

Ba lệnh được sử dụng trên trình chủ NTP và trình khách NTP:

:

```
Router(config)# ntp authenticate
Router(config)# ntp authentication-key key-number md5 key-value
Router(config)# ntp trusted-key key-number
```

Không có cấu hình xác thực NTP, thông tin về thời gian mạng vẫn trao đổi giữa máy chủ và máy khách, nhưng sự khác biệt là các máy khách NTP này không xác thực máy chủ NTP dưới dạng nguồn bảo mật như máy chủ NTP hợp lệ bị hỏng và máy chủ NTP giả mạo vượt qua máy chủ NTP thực.

Điều tra NTP (NTP Enumeration)

Một khía cạnh quan trọng khác của việc thu thập thông tin là thời điểm cụ thể sự kiện xảy ra. Những kẻ tấn công có thể cố gắng thay đổi cài đặt dấu thời gian của bộ định tuyến hoặc có thể giới thiệu máy chủ NTP thô trong mạng để đánh lừa các nhóm pháp y. Nhờ những người sáng tạo của NTP v3, nó có hỗ trợ cho xác thực với máy chủ NTP trước khi xem xét thời gian của mình để được xác thực.

Có thể thu thập thông tin từ NTP bằng các công cụ khác nhau như lệnh NTP, Nmap và một kịch bản NSE. Trong quá trình Điều tra thông qua NTP, kẻ tấn công tạo ra các truy vấn tới máy chủ NTP để trích xuất thông tin có giá trị từ phản hồi như:


- Thông tin máy chủ được kết nối với máy chủ NTP
- Địa chỉ IP của khách hàng, tên máy, thông tin hệ điều hành
- Thông tin mạng như IP nội bộ phụ thuộc vào việc triển khai máy chủ NTP, tức là, nếu máy chủ NTP được triển khai trong DMZ.

Lệnh Điều tra NTP (NTP Enumeration Commands)

ntpdc được sử dụng để truy vấn **ntpd daemon** về trạng thái hiện hành và các thay đổi yêu cầu trong trạng thái.

```
root@kali:~# ntpdc [ -<flag> [<val>] | --<name> [{=| }<val>] ]... [host...]
```

Lệnh ntpdc có thể được sử dụng với các tùy chọn sau:

Tùy chọn	Mô tả
-i	Tùy chọn này buộc phải hoạt động ở chế độ tương tác
-n	Hiển thị địa chỉ máy chủ ở định dạng số bốn chấm
-l	Hiển thị danh sách các đồng nghiệp được biết đến (các) máy chủ.
-p	Hiển thị danh sách các đồng nghiệp được biết đến với máy chủ, ngoài ra, hiển thị tóm tắt trạng thái của họ.
 -s	Hiển thị danh sách các đồng nghiệp được biết đến với máy chủ, bản tóm tắt trạng thái của chúng, ở định dạng khác, tương đương với bộ giảm chấn -c.

ntptrace là một kịch bản Perl, sử dụng ntpq để theo chuỗi các máy chủ NTP từ một máy chủ đã cho trở về nguồn thời gian chính. **ntptrace** yêu cầu thực hiện Giao thức kiểm soát và giám sát NTP được chỉ định trong RFC 1305 và cho phép các gói NTP Mode 6 hoạt động bình thường.

ntpq là một dòng lệnh tiện ích được sử dụng để truy vấn máy chủ NTP. Các **ntpq** được sử dụng để monitor **NTP daemon ntpd** hoạt động & xác định hiệu suất. Nó sử dụng các định dạng tin nhắn điều khiển chuẩn của chế độ NTP 6.

Lệnh **Ntpq** có thể được sử dụng với các tùy chọn sau:

Tùy chọn	Mô tả
-c	Đối số sau đây được hiểu là lệnh định dạng tương tác và được thêm vào danh sách các lệnh được thực thi trên (các) máy chủ được chỉ định. Nhiều tùy chọn -c có thể được cung cấp.
-d	Bật chế độ gỡ lỗi.
-i	Buộc ntpq hoạt động ở chế độ tương tác. Lỗi nhắc sẽ được ghi vào đầu ra tiêu chuẩn và các lệnh đọc từ đầu vào tiêu chuẩn.
-n	Xuất tất cả địa chỉ máy chủ ở định dạng số dotted-quad thay vì chuyển đổi sang tên máy chủ chuẩn.
-p	In danh sách các đồng nghiệp được biết đến với máy chủ cũng như tóm tắt trạng thái của chúng. Điều này tương đương với lệnh tương tác của người ngang hàng.
-4	Buộc phân giải DNS các tên máy chủ sau trên dòng lệnh thành không gian tên IPv4.
-6	Buộc phân giải DNS các tên máy chủ sau trên dòng lệnh thành không gian tên IPv6.

Công cụ Điều tra NTP (NTP Enumeration Tools)

- Nmap
- NTP server Scanner
- Wireshark
- NTPQuery

Điều tra SMTP (SMTP enumeration)

Giao thức chuyển thư đơn giản (SMTP) (Simple Mail Transfer Protocol (SMTP))

SMTP Enumeration là một cách khác để trích xuất thông tin về đích bằng cách sử dụng Giao thức truyền thư đơn giản (SMTP). Giao thức SMTP đảm bảo giao tiếp thư giữa các máy chủ Email và người nhận qua cổng Internet 25. SMTP là một trong những giao thức TCP / IP phổ biến được sử dụng rộng rãi bởi hầu hết các máy chủ email hiện được định nghĩa trong RFC 821.

Kỹ thuật Điều tra SMTP (SMTP Enumeration Technique)

Sau đây là một số lệnh SMTP có thể được sử dụng để Điều tra. Các phản hồi của máy chủ SMTP cho các lệnh này như VRFY, RCPT TO và EXPN là khác nhau. Bằng cách kiểm tra và so sánh các phản hồi cho người dùng hợp lệ và không hợp lệ thông qua tương tác với máy chủ SMTP qua telnet, người dùng hợp lệ có thể được xác định.

Lệnh	Chức năng
HELLO	Để xác định tên miền của người gửi.
EXPN	Xác minh Mailbox trên localhost
MAIL FROM	Để xác định người gửi email.
RCPT TO	Chỉ định người nhận thư.
SIZE	Để chỉ định thông tin kích thước được hỗ trợ tối đa.
DATA	Để xác định dữ liệu.
RSET	Đặt lại kết nối và bộ đệm của SMTP.
VERFY	Xác minh tính khả dụng của máy chủ thư.
HELP	Hiển thị trợ giúp.
QUIT	Để chấm dứt một phiên.



Công cụ Điều tra SMTP (SMTP Enumeration Tool)

- NetScan Tool Pro
- SMTP –user-enum
- Telne

Tính năng chuyển vùng DNS bằng cách sử dụng NSlookup (DNS Zone Transfer Enumeration Using NSlookup)

Trong quá trình điều tra thông qua chuyển vùng DNS, kẻ tấn công tìm thấy cổng TCP của mục tiêu 53, vì cổng TCP 53 được sử dụng bởi DNS và chuyển vùng sử dụng cổng này theo mặc định. Sử dụng kỹ thuật quét cổng, bạn có thể tìm thấy nếu cổng đang mở.

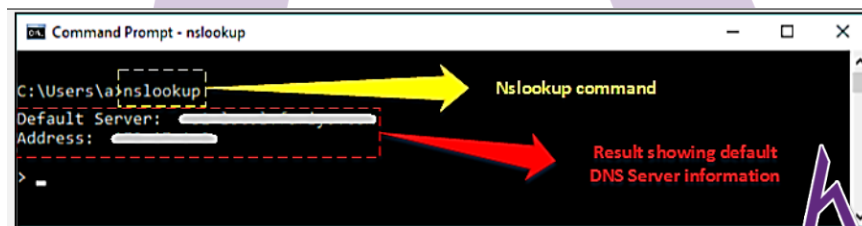
Chuyển vùng DNS (DNS Zone Transfer)

Chuyển vùng DNS là quá trình được thực hiện bởi DNS. Trong quá trình đó, DNS chuyển một bản sao chứa các bản ghi cơ sở dữ liệu đến một máy chủ DNS khác. Quá trình chuyển vùng DNS cung cấp hỗ trợ cho việc giải quyết các truy vấn, vì nhiều máy chủ DNS có thể trả lời các truy vấn.

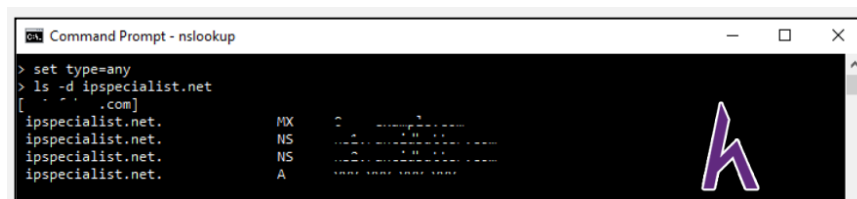
Hãy chú ý một kịch bản trong đó cả máy chủ DNS chính và phụ đều phản hồi các truy vấn. Máy chủ DNS phụ sẽ sao chép bản ghi DNS để cập nhật thông tin trong cơ sở dữ liệu của nó.

Chuyển vùng DNS bằng lệnh Nslookup

1. Truy cập dòng lệnh **Windows (CMD)** và nhập **Nslookup** và nhấn **Enter**.

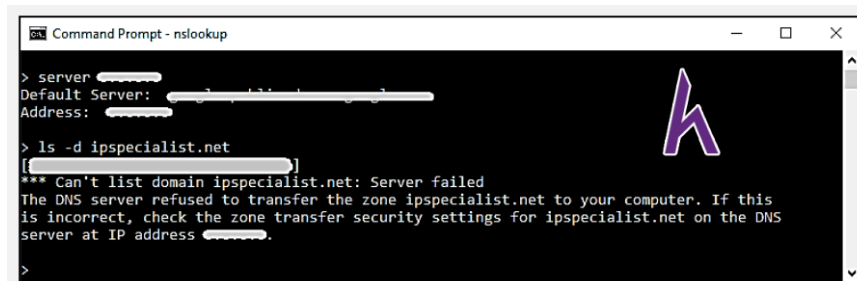


2. Command prompt will proceed to " > " symbol.
3. Enter " server <DNS Server Name> " or " server <DNS Server Address> ".
4. Enter set type=any and press Enter. It will retrieve all records from a DNS server.
5. Enter ls -d <Domain> this will display the information from the target domain (if allowed).



```
Command Prompt - nslookup
> set type=any
type=any
> ls -d ipspecialist.net
[ . . . .com]
ipspecialist.net.      MX      10      10.10.10.10
ipspecialist.net.      NS      1      10.10.10.10
ipspecialist.net.      NS      2      10.10.10.10
ipspecialist.net.      A       1      10.10.10.10
```

6. If not allowed, it will show the request failed



```
Command Prompt - nslookup
> server [redacted]
Default Server: [redacted]
Address: [redacted]
> ls -d ipspecialist.net
*** Can't list domain ipspecialist.net: Server failed
The DNS server refused to transfer the zone ipspecialist.net to your computer. If this
is incorrect, check the zone transfer security settings for ipspecialist.net on the DNS
server at IP address [redacted].
>
```

7. Linux support dig command, At a command prompt enter dig <domain.com> axfr.

Biện pháp đối phó Điều tra (Enumeration Countermeasures)

Sử dụng kỹ thuật bảo mật nâng cao, phần mềm bảo mật nâng cao, phiên bản cập nhật của giao thức, chính sách bảo mật công hiệu, mật khẩu đa dạng và khó khăn, giao tiếp mã hóa mạnh mẽ giữa máy khách và máy chủ, vô hiệu hóa các cổng không cần thiết, giao thức, chia sẻ và dịch vụ kích hoạt mặc định có thể ngăn chặn việc Điều tra cấp độ.

Sơ đồ tư duy