COMP 4632
Practicing Cybersecurity: Attacks and Counter-measures

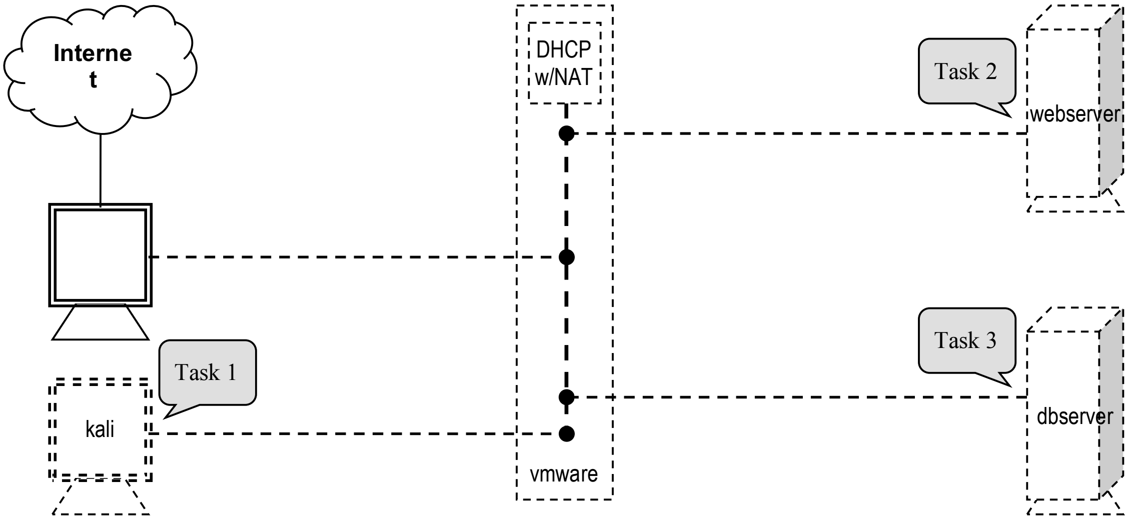
Week 3 Lab Exercise

Topic: *System Infrastructure*

Lab Objective

In this lab, we are going to let you gain experience on the server setup in a virtualized environment by walking through the configuration procedure of Linux servers. In the future, you will try to perform information gathering via vulnerability scanning on those servers. The whole setup will include the following components:

- Vulnerability Scanner Configuration
- CentOS Linux Installation Walkthrough
- Apache Web Server Configuration
- vsFTP File Server Configuration
- Bind Domain Name Server Configuration
- MySQL Database Server Configuration



****Note: The infrastructure setup in this lab will be used in the labs in coming few weeks. If you cannot follow or encounter any issues, please do not hesitate to seek help from TA.***

Task 1 – Prepare Kali Linux Client

Before initiating a vulnerability scan, it is necessary to understand the configuration of a vulnerability scanner and enable appropriate plugin so that the information gathering could be performed effectively. In this task, we will walk through the setup and plugin update of the scanner. The scanning will be initiated in task 3.

Task 1.1 Install VMware Tools in Kali Linux

- Turn on the Kali Linux Virtual Machine
- In the VMware Player, select Player → Manage → Install VMware Tools
- Install VMware Tools using the following command and use default options during the installation

```
mount /dev/cdrom /mnt/hgfs
cd /tmp
tar zxf /mnt/hgfs/VMwareTools-9.9.3-<xxxxxxx>.tar.gz
umount /dev/cdrom
cd vmware-tools-distrib
./vmware-install.pl
```

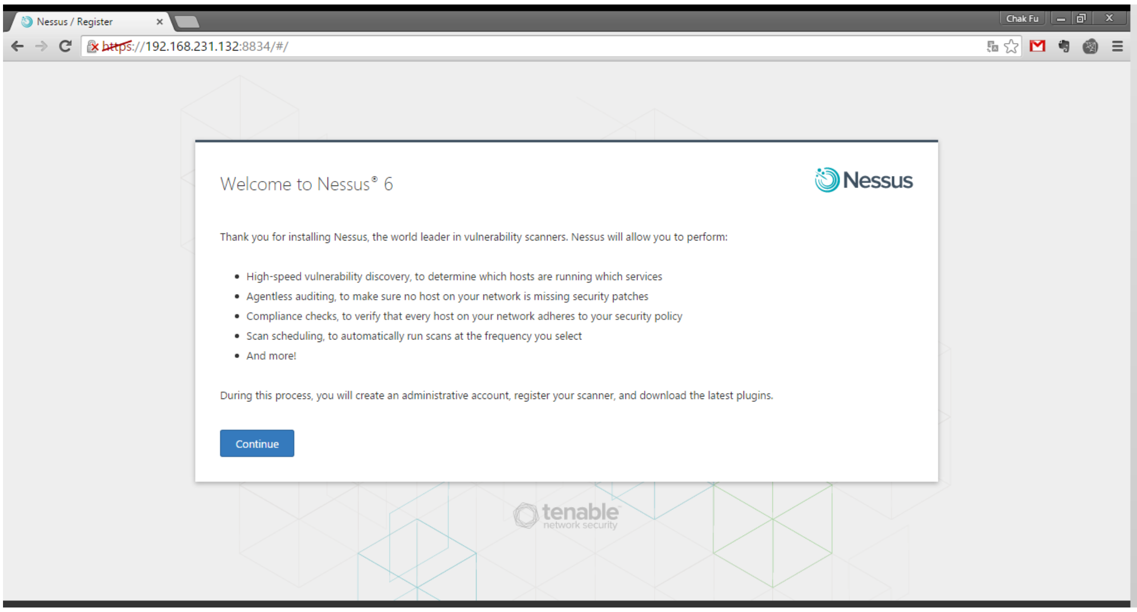
- You will be able to drag and drop files to the guest machine now

Task 1.2 Install and activate Nessus 6.4.0

- Drag and drop the Nessus-6.4.0-debian6_amd64.deb file into Kali Linux
- Install Nessus 6.4.0 using the following command

```
dpkg -i Nessus-6.4.0-debian6_amd64.deb
/etc/init.d/nessusd start
```

- Access the Nessus web interface via https://<kali_linux_ip>:8834



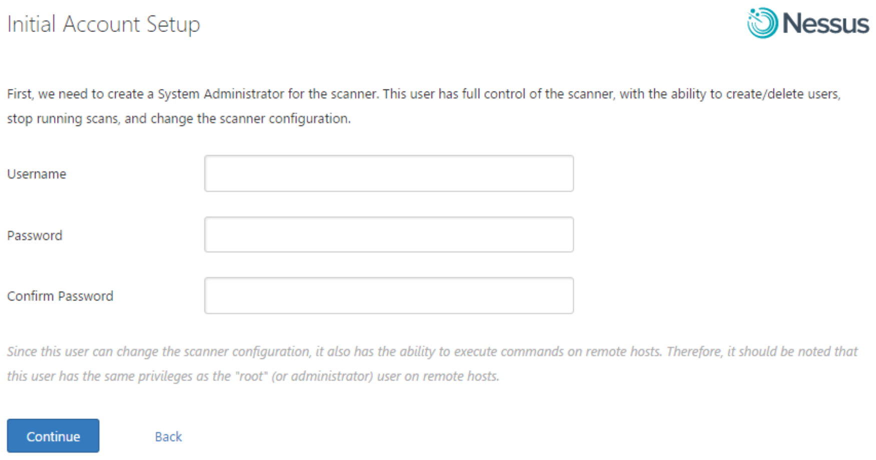
Welcome to Nessus® 6

Thank you for installing Nessus, the world leader in vulnerability scanners. Nessus will allow you to perform:

- High-speed vulnerability discovery, to determine which hosts are running which services
- Agentless auditing, to make sure no host on your network is missing security patches
- Compliance checks, to verify that every host on your network adheres to your security policy
- Scan scheduling, to automatically run scans at the frequency you select
- And more!

During this process, you will create an administrative account, register your scanner, and download the latest plugins.

- Create a Nessus user account:
  - Username: comp4632
  - Password: pass4632



Initial Account Setup

First, we need to create a System Administrator for the scanner. This user has full control of the scanner, with the ability to create/delete users, stop running scans, and change the scanner configuration.

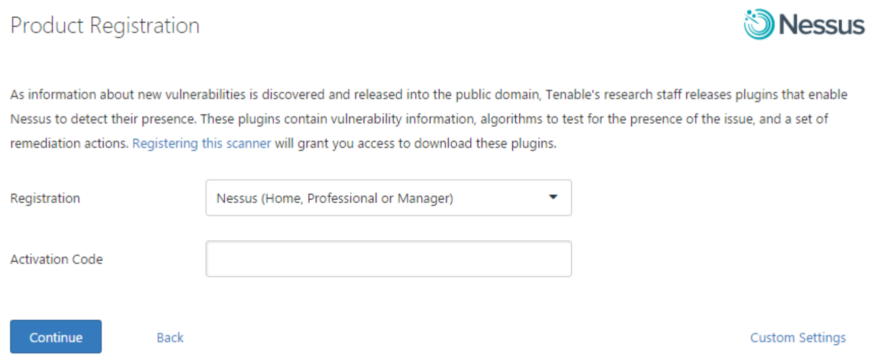
Username

Password

Confirm Password

Since this user can change the scanner configuration, it also has the ability to execute commands on remote hosts. Therefore, it should be noted that this user has the same privileges as the "root" (or administrator) user on remote hosts.

- An activation code would be required for the product registration



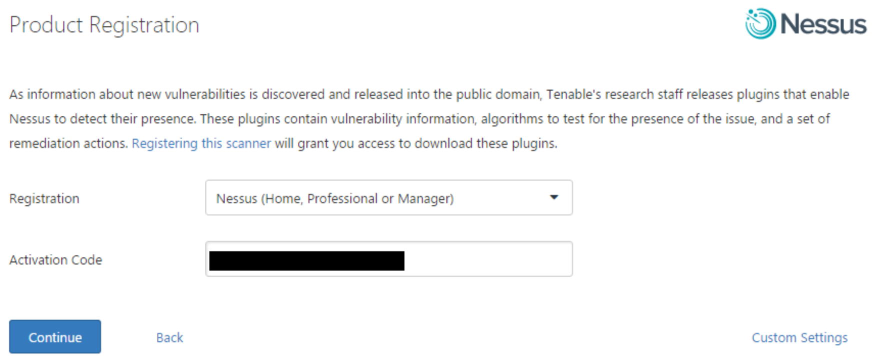
Product Registration

As information about new vulnerabilities is discovered and released into the public domain, Tenable's research staff releases plugins that enable Nessus to detect their presence. These plugins contain vulnerability information, algorithms to test for the presence of the issue, and a set of remediation actions. Registering this scanner will grant you access to download these plugins.

Registration: Nessus (Home, Professional or Manager)

Activation Code:

- Register for an activation code in the Nessus website
  - https://www.tenable.com/products/nessus-home
- An email containing the activation code would be sent to your email address
- Select "Nessus (Home, Professional or Manager)" and enter the activation code in the Nessus web interface



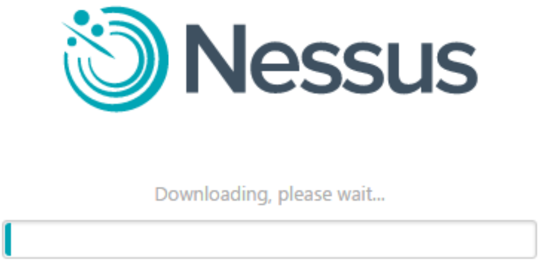
Product Registration

As information about new vulnerabilities is discovered and released into the public domain, Tenable's research staff releases plugins that enable Nessus to detect their presence. These plugins contain vulnerability information, algorithms to test for the presence of the issue, and a set of remediation actions. Registering this scanner will grant you access to download these plugins.

Registration: Nessus (Home, Professional or Manager)

Activation Code: [redacted]

- Nessus will automatically update the plugin and perform initialization



Downloading, please wait...

Task 2 – Public Accessible Multi-purpose Web Server

In this task, we will walk through the configuration of Web server, FTP server and DNS server. You are expected to understand the basic concept of each server by experiencing these setups.

Task 2.1 Understanding Linux System

- Unzip the given 64-bit Linux VM "CentOS5.11.zip" into D:\comp4632\Users\
- Power on the virtual machine
- Login as "root" with password "admin123"

- Type in the following commands and answer questions 1~3

```
pwd
ls
shutdown -r now
netstat -tulanp
ifconfig
shutdown -h now
```

## Question 1: It is important to know where your command is typed. What is the full path when you type `ls` as above? (0.5 mark)

## Question 2: What ports are opened in the server? (0.5 mark)

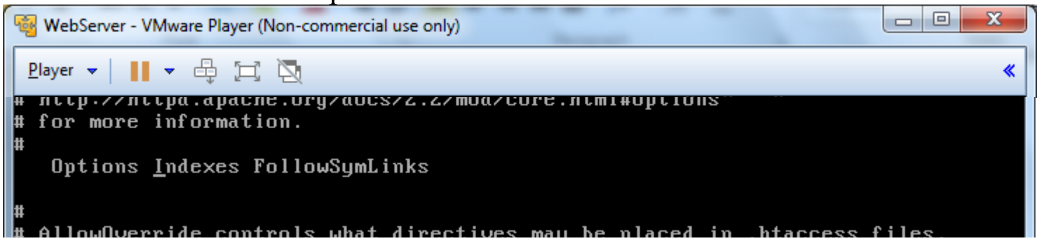
## Question 3: What is the IP address of this server? (1 mark) Please note that it will be used in the subsequent configuration steps.

Task 2.2 Configuring Web Server

- Type the following command to edit the Apache config file

```
vi /etc/httpd/conf/httpd.conf
```

- Type320G to go to line 320
- Move the cursor to the capital letter I as shown below



```
# http://httpd.apache.org/docs/2.2/mod/core.html#options
# for more information.
#
    Options Indexes FollowSymLinks

#
# AllowOverride controls what directives may be placed in .htaccess files.
```

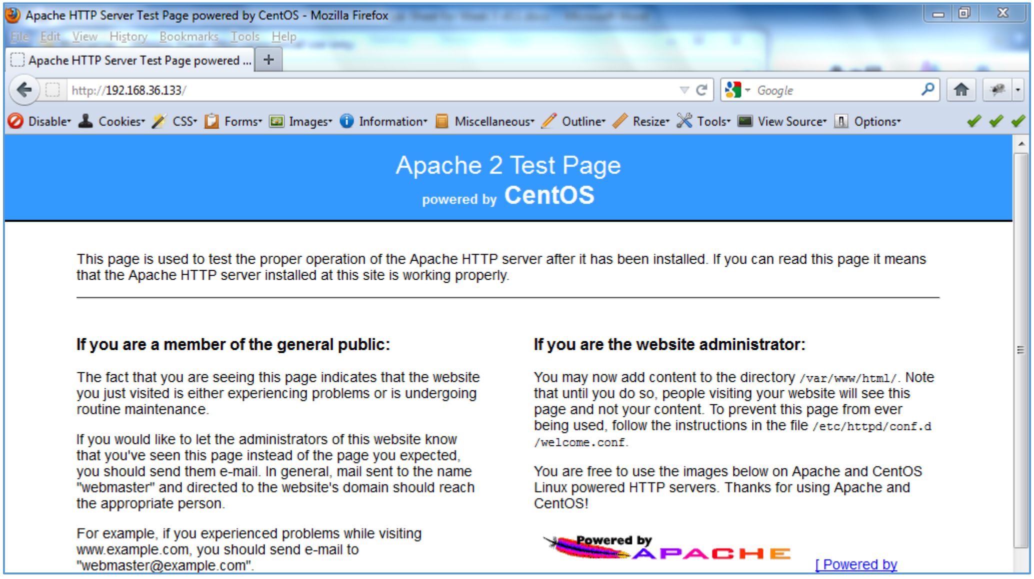
- Type xxxxxxxx to delete the word “Indexes”

## Bonus Question 1: What is the purpose of deleting the key word “Indexes” in the config file? (1 mark)

- Type :wq and press Enter to save changes and quit editing
- Start the HTTP daemon with the following command

```
service httpd start
```

- Try accessing web server in a client browser using IP address, such as



Apache HTTP Server Test Page powered by CentOS - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Apache HTTP Server Test Page powered ...
http://192.168.36.133/
Google
Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options
Powered by APACHE

Apache 2 Test Page
powered by CentOS

This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page it means that the Apache HTTP server installed at this site is working properly.

If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

If you are the website administrator:

You may now add content to the directory `/var/www/html/`. Note that until you do so, people visiting your website will see this page and not your content. To prevent this page from ever being used, follow the instructions in the file `/etc/httpd/conf.d/welcome.conf`.

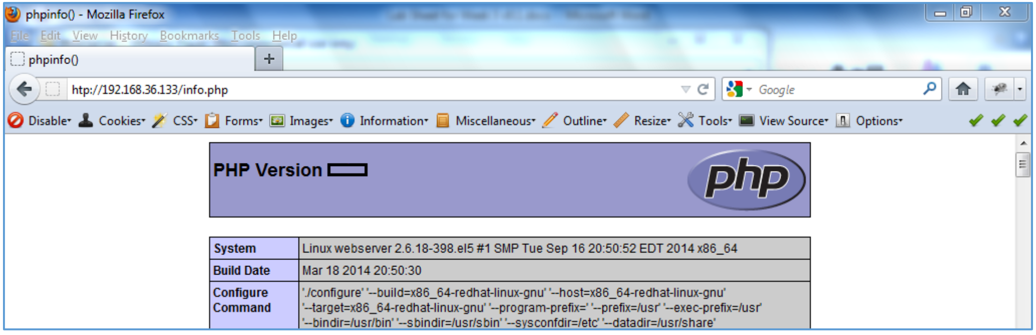
You are free to use the images below on Apache and CentOS Linux powered HTTP servers. Thanks for using Apache and CentOS!

[Powered by

- Test the PHP module by creating a simple web page

```
echo '<?php phpinfo(); ?>' >/var/www/html/info.php
```

- Again, try accessing this new page in client browser


phpinfo() - Mozilla Firefox
File Edit View History Bookmarks Tools Help
phpinfo()
+
Google
Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options
php

http://192.168.36.133/info.php

PHP Version [redacted]

System	Linux webserver 2.6.18-398.el5 #1 SMP Tue Sep 16 20:50:52 EDT 2014 x86_64
Build Date	Mar 18 2014 20:50:30
Configure Command	'./configure' '--build=x86_64-redhat-linux-gnu' '--host=x86_64-redhat-linux-gnu' '--target=x86_64-redhat-linux-gnu' '--program-prefix=' '--prefix=/usr' '--exec-prefix=/usr' '--bindir=/usr/bin' '--sbindir=/usr/sbin' '--sysconfdir=/etc' '--datadir=/usr/share'

## Question 4: What is the PHP version shown on the page? (0.5 mark)

- Adding additional PHP extensions for MySQL database and GD image libraries

```
yum install php-mysql php-gd
```

- Answer Y for all of the questions and restart Apache daemon afterwards

```
service httpd restart
```

- Finally, setting the daemon to start up at boot time

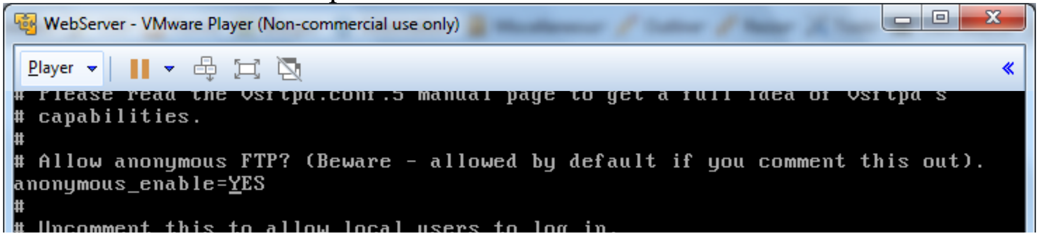
```
chkconfig --level 3 httpd on
```

Task 2.3 Configuring FTP Server

- Type the following command to edit the vsFTP config file

```
vi /etc/vsftpd/vsftpd.conf
```

- Type 12G to go to line 12
- Move the cursor to the capital letter Y as shown below



```
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
# Allow anonymous FTP? (Beware - allowed by default if you comment this out).
anonymous_enable=YES
#
# Uncomment this to allow local users to log in.
```

- Type i to text insert mode
- Type NO to disable anonymous login
- Press **Esc** to back to command mode
- Move the cursor to the capital letter Y again
- Type xxx to delete the word "YES"
- Type 115G to go to line 115
- Type i to text insert mode
- Type pasv_enable=YES to enable passive mode
- Press **Esc** to back to command mode
- Type :wq and press **Enter** to save changes and quit editing
- Create a FTP account "comp4632" with password "pass4632" so that user can upload home pages to the web directory

```
useradd -g50 -d/var/www/html -s/sbin/nologin
comp4632
passwd comp4632
pass4632
pass4632
chown -R comp4632:ftp /var/www/html
```

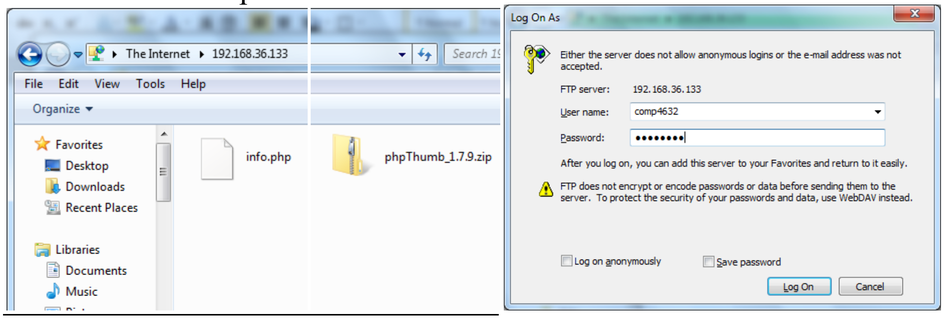
- Start the vsFTP daemon with the following command

```
service vsftpd start
```

- Try login to the FTP account, then test downloading the file “info.php” and uploading the provided file “phpThumb_1.7.9.zip”
  - from Terminal of Kali Linux Client

```
cd /tmp
ftp 192.168.36.139
comp4632
pass4632
quote pasv
asc
get info.php
bin
put phpThumb_1.7.9.zip
ls
bye
```

  - from Windows Explorer



Either the server does not allow anonymous logins or the e-mail address was not accepted.

FTP server: 192.168.36.133

User name: comp4632

Password: ••••••••

After you log on, you can add this server to your Favorites and return to it easily.

FTP does not encrypt or encode passwords or data before sending them to the server. To protect the security of your passwords and data, use WebDAV instead.

□ Log on anonymously □ Save password

- Unzip the file to check whether it is really successfully uploaded

```
cd /var/www/html
unzip -dphpThumb_1.7.9 phpThumb_1.7.9.zip
```

- Finally, setting the daemon to start up at boot time

```
chkconfig --level 3 vsftpd on
```

Task 2.4 Configuring DNS Server

- **[Warning]** Remember to use your own IP obtained in Question #3 to configure DNS, and don’t just copy and paste blindly without knowing what you are actually doing!
- Type the following command to edit the ***global config file***

```
vi /var/named/chroot/etc/named.conf
```

  - Type i to text insert mode
  - Type (or copy and paste) the following content

```
options {
    allow-transfer {
        none;
    };
    allow-query {
        any;
    };
    forwarders {
        192.168.36.2;
    };
    recursion yes;
};
```

```
include "/etc/named.conf.local";
```

- Press Esc to back to command mode
- Type :wq and press Enter to save changes and quit editing
- (Optional) Check the syntax of the config file

```
named-checkconf -t/var/named/chroot /etc/named.conf
```

- Type the following command to edit the ***local config file***

```
vi /var/named/chroot/etc/named.conf.local
```

  - Type i to text insert mode
  - Type (or copy and paste) the following content

```
zone "." IN {
    type hint;
    file "../var/named/data/named.root";
};
zone "8win.com" IN {
    type master;
    file "../var/named/data/named.8win.com";
};
zone "36.168.192.in-addr.arpa" IN {
    type master;
    file "../var/named/data/named.192.168.36";
};
```

  - Press Esc to back to command mode
  - Type :wq and press Enter to save changes and quit editing
  - (Optional) Check the syntax of the config file

```
named-checkconf -t/var/named/chroot /etc/named.conf.local
```

- Download from InterNIC the official ***root zone file***

```
cd /var/named/chroot/var/named/data
wget 'ftp://rs.internic.net/domain/named.root'
```

- Type the following command to edit the ***forward zone file***

```
vi /var/named/chroot/var/named/data/named.8win.com
```

  - Type i to text insert mode
  - Type (or copy and paste) the following content (note that any unused IP within the same subnet can be temporary assigned to the A record of dbserver and it will be fixed later)

```
$TTL 3H
@ IN SOA   ns1.8win.com. info.8win.com. (
    201509011500   ; Serial
    30M            ; Refresh
    10M            ; Retry
    3D             ; Expire
    1H )           ; Negative Cache TTL

; Name Servers - NS Records
```

```
@                   IN NS    ns1.8win.com.

; Name Servers - A Records
ns1.8win.com.       IN A     192.168.36.139

; Servers - A Records
webserver.8win.com. IN A     192.168.36.139
dbserver.8win.com.  IN A     192.168.36.140

; Servers - CNAME Records
www                 IN CNAME
webserver.8win.com.
ftp                 IN CNAME
webserver.8win.com.
db                  IN CNAME dbserver.8win.com.
```

- Press Esc to back to command mode
- Type :wq and press Enter to save changes and quit editing
- (Optional) Check the syntax of the zone file

```
cd /var/named/chroot/var/named/data
named-checkzone 8win.com named.8win.com
```

- Type the following command to edit the ***reverse zone file***

```
vi /var/named/chroot/var/named/data/named.192.168.36
```

  - Type i to text insert mode
  - Type (or copy and paste) the following content

```
$TTL 3H
@ IN SOA  ns1.8win.com. info.8win.com. (
    201509011500   ; Serial
    30M            ; Refresh
    10M            ; Retry
    3D             ; Expire
    1H )           ; Negative Cache TTL

; Name Servers - NS Records
@                   IN NS    ns1.8win.com.

; PTR Records
139                 IN PTR
webserver.8win.com.
140                 IN PTR   dbserver.8win.com.
```

  - Press Esc to back to command mode
  - Type :wq and press Enter to save changes and quit editing
  - (Optional) Check the syntax of the zone file

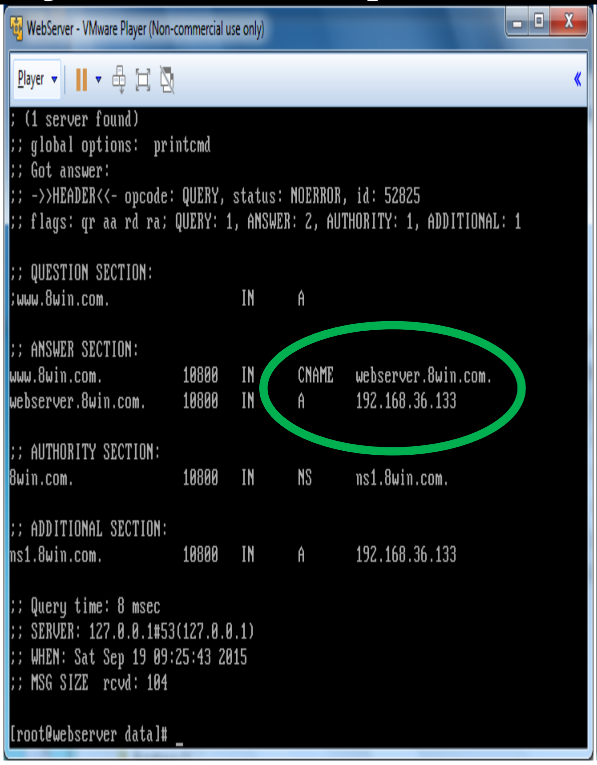
```
cd /var/named/chroot/var/named/data
named-checkzone 8win.com named.192.168.36
```

- Start the NAME daemon with the following command

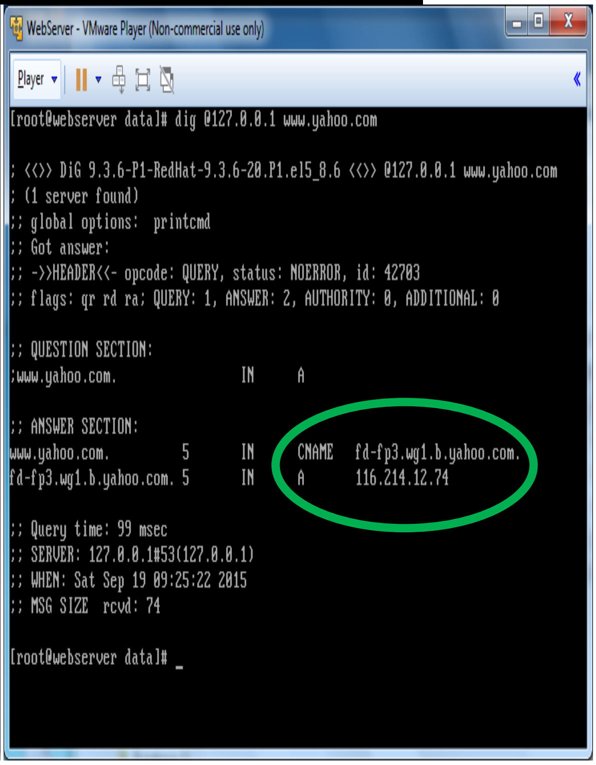
```
service named start
```

- Test looking up of internal and external domains

```
dig @127.0.0.1 www.8win.com
dig @127.0.0.1 www.yahoo.com
```



```
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52825
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;www.8win.com.                  IN      A

;; ANSWER SECTION:
www.8win.com.           10800   IN      CNAME   webserver.8win.com.
webserver.8win.com.     10800   IN      A       192.168.36.133

;; AUTHORITY SECTION:
8win.com.               10800   IN      NS      ns1.8win.com.

;; ADDITIONAL SECTION:
ns1.8win.com.           10800   IN      A       192.168.36.133

;; Query time: 8 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sat Sep 19 09:25:43 2015
;; MSG SIZE  rcvd: 104

[root@webserver data]# _
```

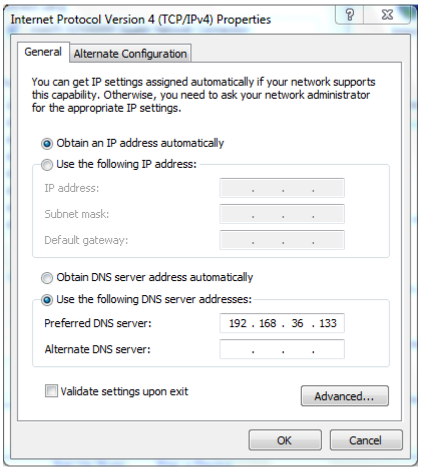


```
[root@webserver data]# dig @127.0.0.1 www.yahoo.com

; <<>> DiG 9.3.6-P1-RedHat-9.3.6-20.P1.el5_8.6 <<>> @127.0.0.1 www.yahoo.com
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42703
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.yahoo.com.                 IN      A

;; ANSWER SECTION:
www.yahoo.com.          5       IN      CNAME   fd-fp3.wg1.b.yahoo.com.
fd-fp3.wg1.b.yahoo.com. 5       IN      A       116.214.12.74

;; Query time: 99 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sat Sep 19 09:25:22 2015
;; MSG SIZE  rcvd: 74

[root@webserver data]# _
```

- Finally, setting the daemon to start up at boot time

```
chkconfig --level 3 named on
```

- Configure all clients to lookup this DNS server and test them
    - in Windows client

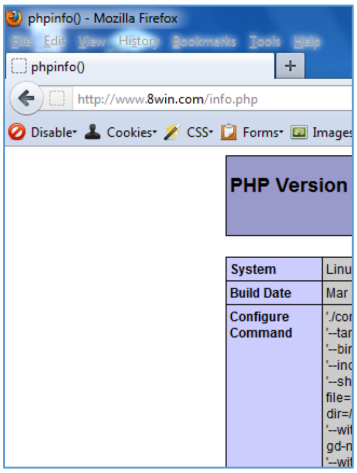


You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address: . . .
Subnet mask: . . .
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 36 . 133
Alternate DNS server: . . .

□ Validate settings upon exit


phpinfo() - Mozilla Firefox
File Edit View History Bookmarks Tools Help
phpinfo()
Disable
Cookies
CSS
Forms
Images

http://www.8win.com/info.php

PHP Version

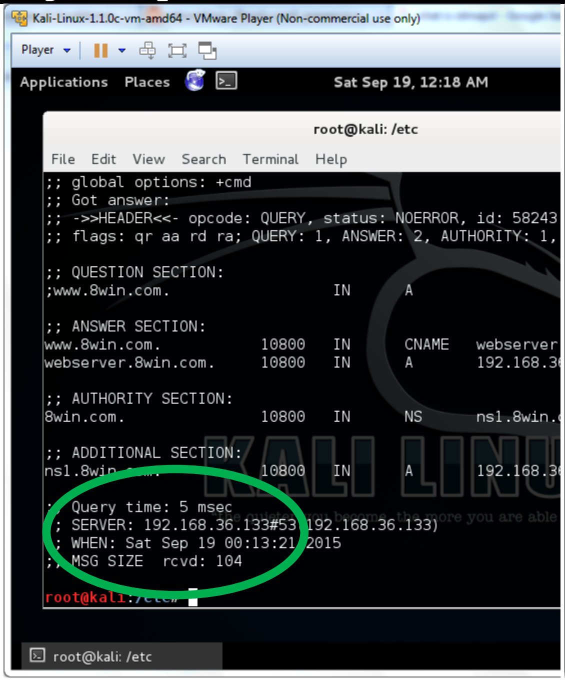
System	Linu
Build Date	Mar
Configure Command	'./co '--tar '--bir '--inc '--sh file= dir=/ '--wi gd-n '--wi

- in CentOS/RHEL/RedHat Linux client

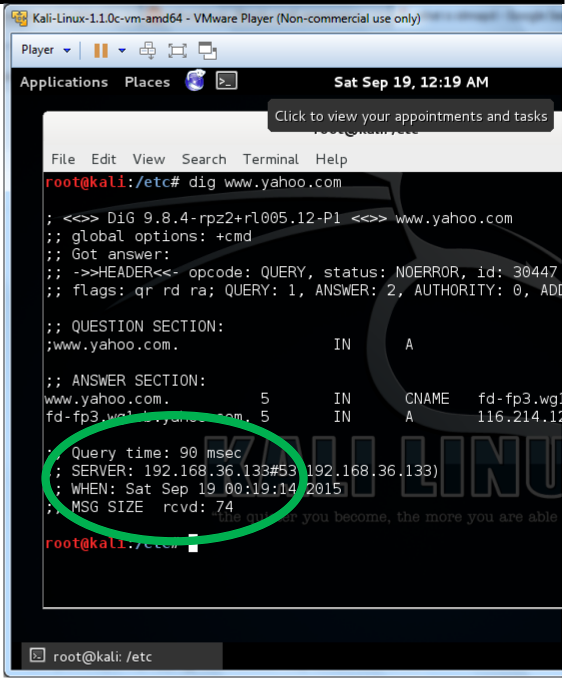
```
ifdown eth0
echo 'PEERDNS=no' >>/etc/sysconfig/network-scripts/ifcfg-eth0
ifup eth0
echo 'search 8win.com' >/etc/resolv.conf
echo 'nameserver 192.168.36.139' >>/etc/resolv.conf
dig www.8win.com
dig www.yahoo.com
```

- in Kali/Ubuntu/Debian Linux client

```
echo 'supersede domain-search "8win.com";' >>
                                      /etc/dhcp/dhclient.conf
echo 'supersede domain-name-servers 192.168.36.139;' >>
                                      /etc/dhcp/dhclient.conf
shutdown -r now
dig www.8win.com
dig www.yahoo.com
```



```
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58243
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 1,

;; QUESTION SECTION:
;www.8win.com.                  IN      A

;; ANSWER SECTION:
www.8win.com.           10800   IN      CNAME   webserver
webserver.8win.com.     10800   IN      A       192.168.3

;; AUTHORITY SECTION:
8win.com.               10800   IN      NS      ns1.8win.

;; ADDITIONAL SECTION:
ns1.8win.com.           10800   IN      A       192.168.3

;; Query time: 5 msec
;; SERVER: 192.168.36.133#53(192.168.36.133)
;; WHEN: Sat Sep 19 00:13:21 2015
;; MSG SIZE  rcvd: 104

root@kali:/etc#
```


Kali-Linux-1.1.0c-vm-amd64 - VMware Player (Non-commercial use only)
Player
Applications
Places
Sat Sep 19, 12:19 AM
Click to view your appointments and tasks
File
Edit
View
Search
Terminal
Help

```
root@kali:/etc# dig www.yahoo.com

; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> www.yahoo.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30447
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADD

;; QUESTION SECTION:
;www.yahoo.com.                 IN      A

;; ANSWER SECTION:
www.yahoo.com.          5       IN      CNAME   fd-fp3.wg1
fd-fp3.wg1.b.yahoo.com. 5       IN      A       116.214.12

;; Query time: 90 msec
;; SERVER: 192.168.36.133#53(192.168.36.133)
;; WHEN: Sat Sep 19 00:19:14 2015
;; MSG SIZE  rcvd: 74

root@kali:/etc#
```

Task 3 – Backend Database Server

This task will let you prepare a database server for vulnerability scan before and after its configuration hardening.

Task 3.1 Install Linux Server for Database

- Create another CentOS 64-bit VM for DbServer via either one of the following ways (with the first one recommended):
  - Create the VM from scratch using the steps specified in the installation walkthrough slides (remember to use "dbserver" as the hostname); or
  - (Just A Quick Alternative) Unzip another VM from the original given image (refer to **Task 2.1**), and temporary change the hostname to "dbserver" with the `` `hostname dbserver` `` command, but this change has 2 problems:
    1. the display name will not follow the changed hostname
    2. the change is not permanent and will lost after reboot

  ## Bonus Question 2: How is the output of `` `fdisk -l` `` command in DbServer different from WebServer? (2 marks)
- Start the MySQL daemon with the following command

```
service mysqld start
```

- Set the daemon to start up at boot time

```
chkconfig --level 3 mysqld on
```

Task 3.2 Configure MySQL to Allow Remote Connection

- Power on the CentOS5.11 database server virtual machine
- Configure the MySQL to allow remote access from any machine

```
mysql -uroot
SHOW DATABASES;
USE mysql;
UPDATE user SET host='%' WHERE host<>'localhost' AND
host<>'127.0.0.1' AND user='root';
FLUSH PRIVILEGES;
\q
```

## Question 5: What databases are created by default? (0.5 mark)

- Remember to fix A record and PTR record of “dbserver.8win.com” in the two zone files at WebServer
- Also remember to configure this database server to lookup DNS which was ready in Task 2.4 as well

---

End of Lab