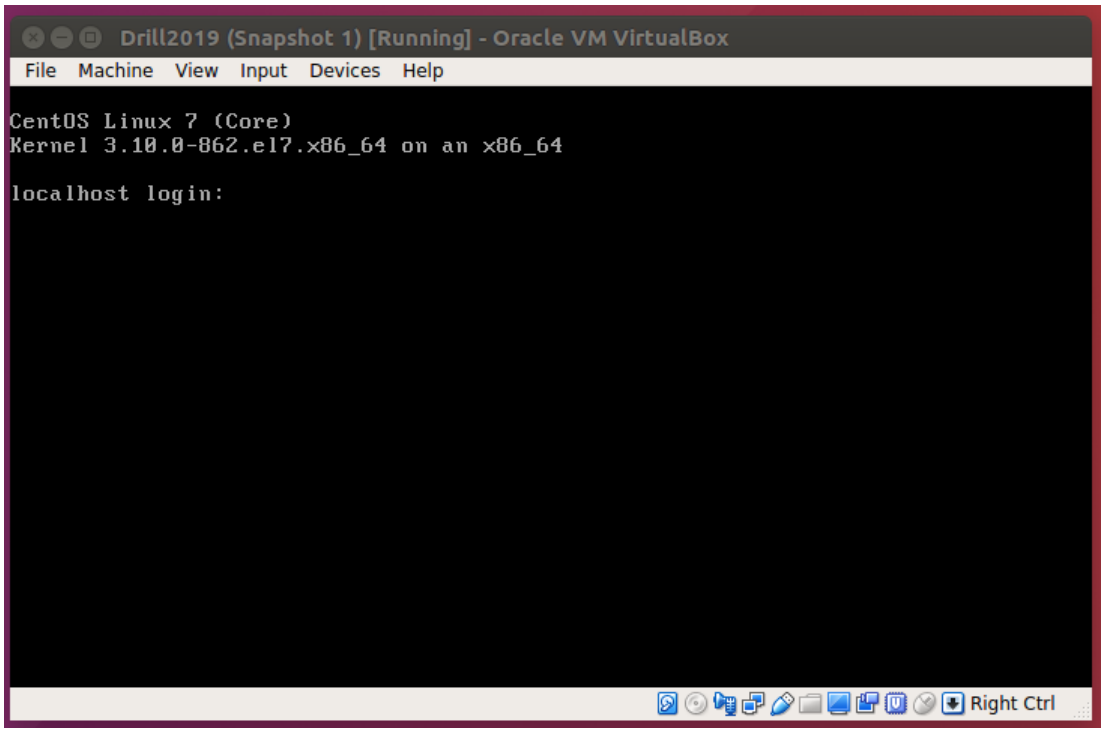
[Write-Up] Cyber Security Drill Test Sektor Pemerintah 2019 : Case Insiden Web Defacement

A. Persiapan Sistem

1. Menyiapkan environment simulasi

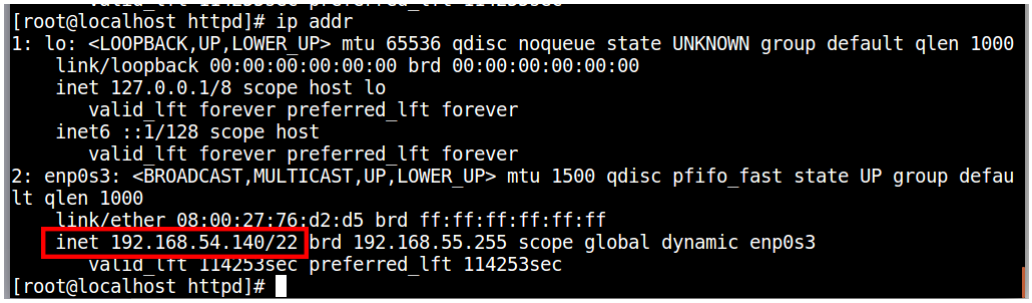
Environment yang digunakan dalam melakukan simulasi adalah menggunakan sistem Virtualization yang dapat dilakukan instalasi pada PC atau Laptop. Siapkan sistem Virtualization yang dapat digunakan, contoh : VirtualBox (https://www.virtualbox.org/wiki/Downloads). Lalu siapkan ISO web server yang terkena insiden Web Defacement, dapat diunduh di link :
https://s.id/isoDrill2019 (*password* : dr11lbs5n2019)
Buka ISO tersebut pada VirtualBox yang telah diunduh (tutorial : https://techathlon.com/how-to-run-a-vmdk-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
```



Gambar 2. Alamat IP Server.

Untuk memeriksa bahwa pengaturan sudah sesuai, perlu diperiksa pada browser anda dengan mengetikan 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

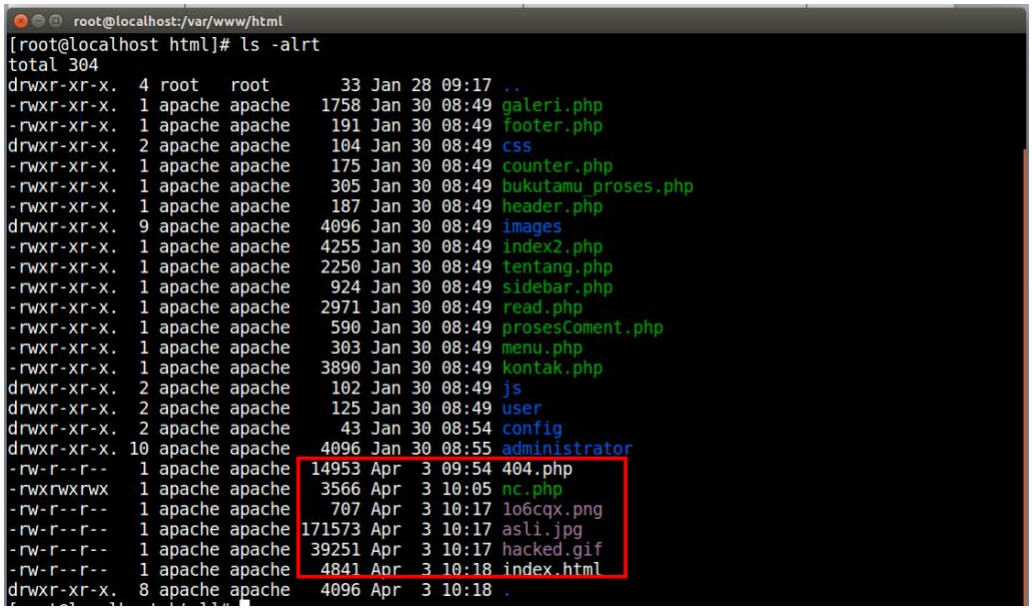
Dalam melakukan penanganan insiden ini, yang dilakukan adalah melakukan proses identifikasi dan analisis insiden. Identifikasi insiden merupakan proses penanganan insiden yang dilakukan dengan mengumpulkan bukti-bukti insiden seperti screnshot defacement, bukti malicious file, bukti malicious activity,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

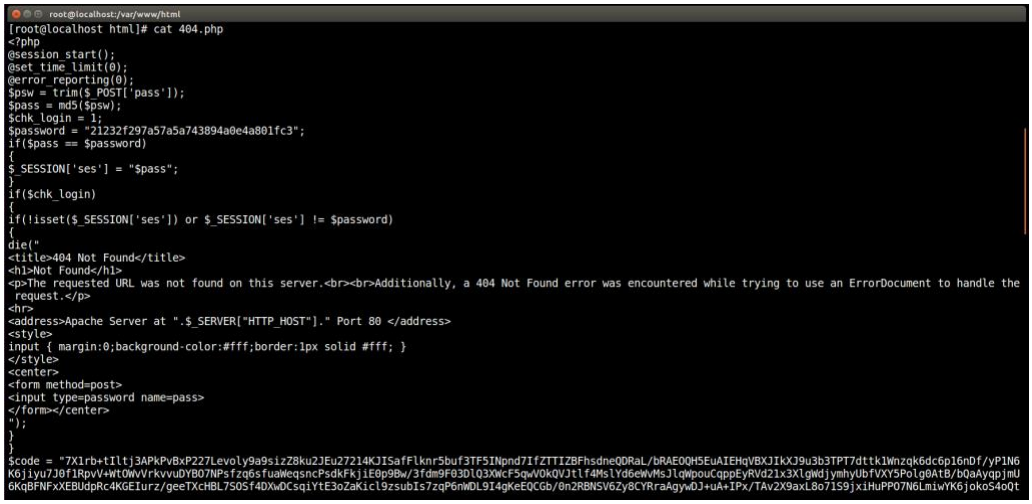
```
# ls -alrt /var/www/html/
```



Gambar 4. Daftar *file* pada *home directory website*.

Berdasarkan hasil identifikasi, terdapat 6 file yang diindikasikan merupakan malicious file yaitu nc.php, 404.php, 1o6cqx.png, hacked.gif, dan asli.png. Untuk memeriksa setiap file dapat menggunakan tools viewer atau editor linux.

```
# cat 404.php
```

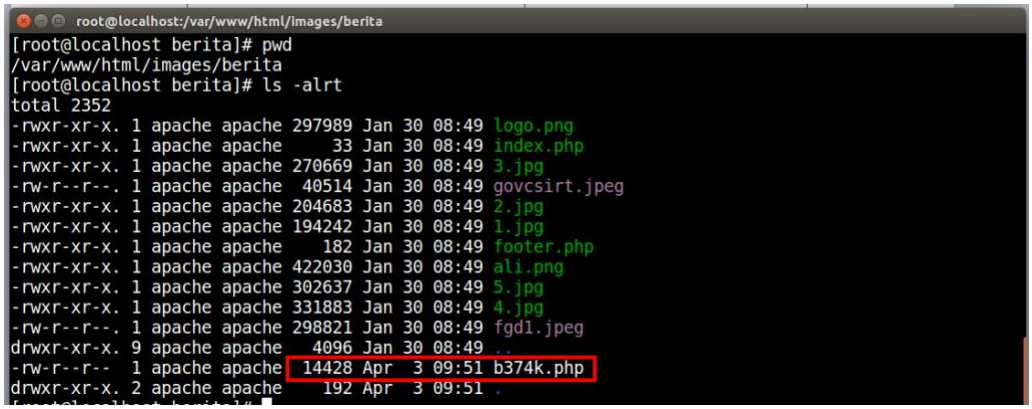


Gambar 5. *Preview* dari *malicious file.*

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

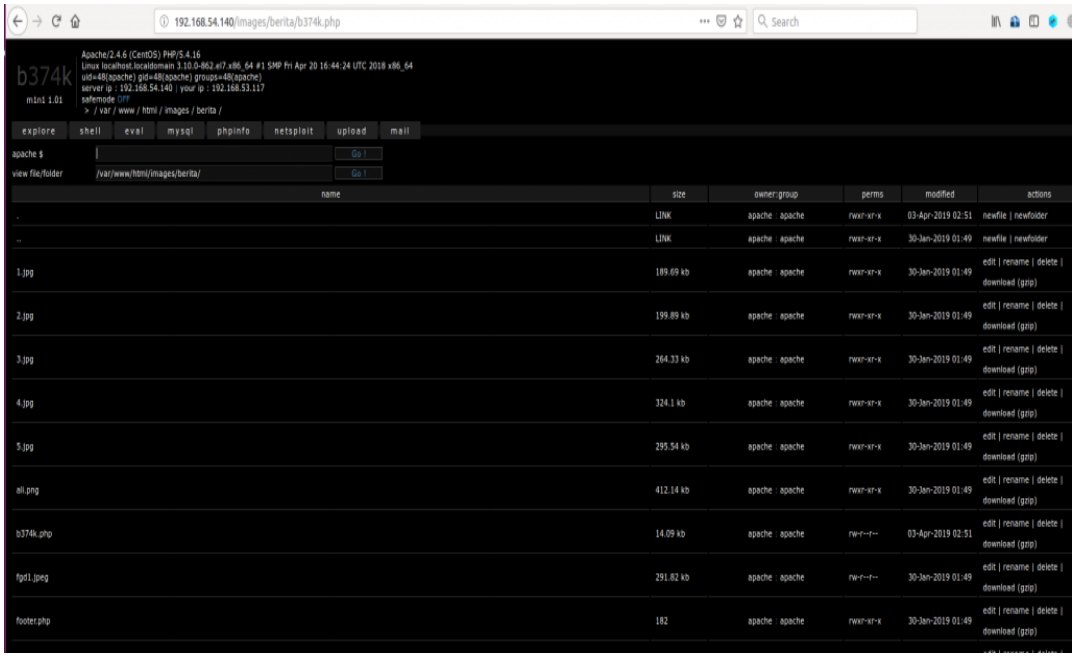
2. Periksa *public directory*

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*.



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

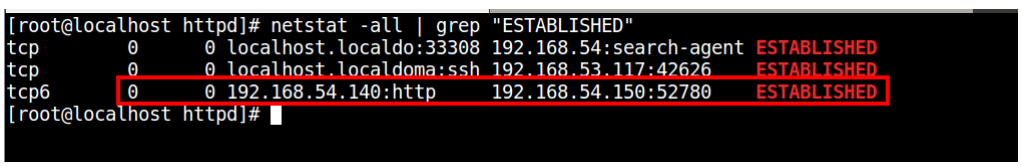
Selanjutnya adalah memeriksa kondisi jaringan pada server, periksa apakah terdapat koneksi yang bersifat malicious atau tidak. Command yang dapat dilakukan adalah :

`# netstat -tulnp` [menampilkan koneksi outbound]

`# netstat -antp` [menampilkan koneksi tcp inbound]

`# nestat -anup` [menampilkan koneksi udp inbound] Jika untuk mengetahui malicious koneksi yang masih aktif, dapat melakukan command sebagai berikut :

`# nestat -all | grep "ESTABLISHED"` [menampilkan koneksi yang aktif]



Gambar 8. Daftar koneksi yang aktif.

4. Periksa history command

Selanjutnya periksa history command yang digunakan dengan memeriksa file ~/.bash_history

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

```
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/sshd:/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]#
```

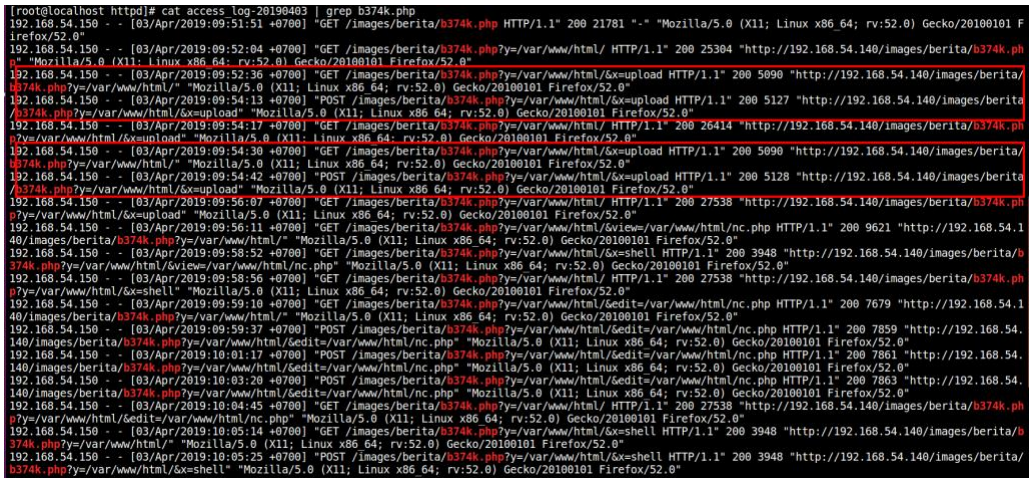
Gambar 10. Daftar *user.*

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/.

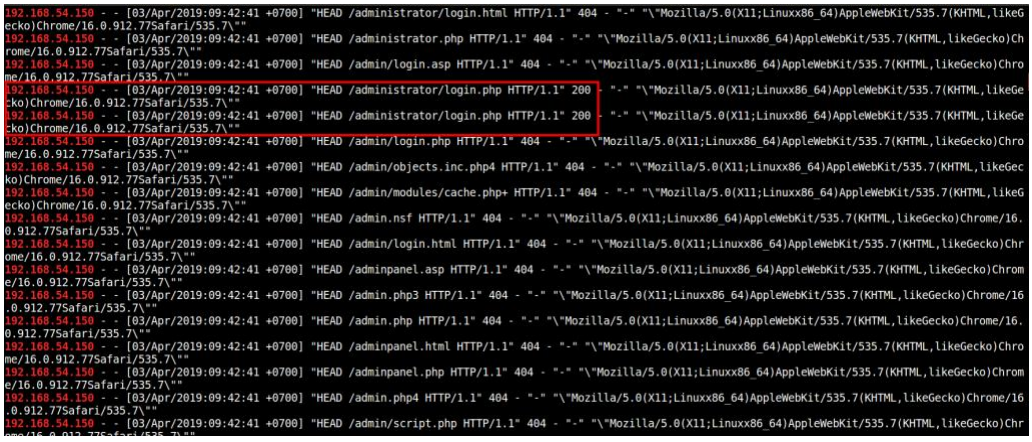
Trik sederhana dalam melakukan analisis log jika ditemukan backdoor adalah sebagai berikut :

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



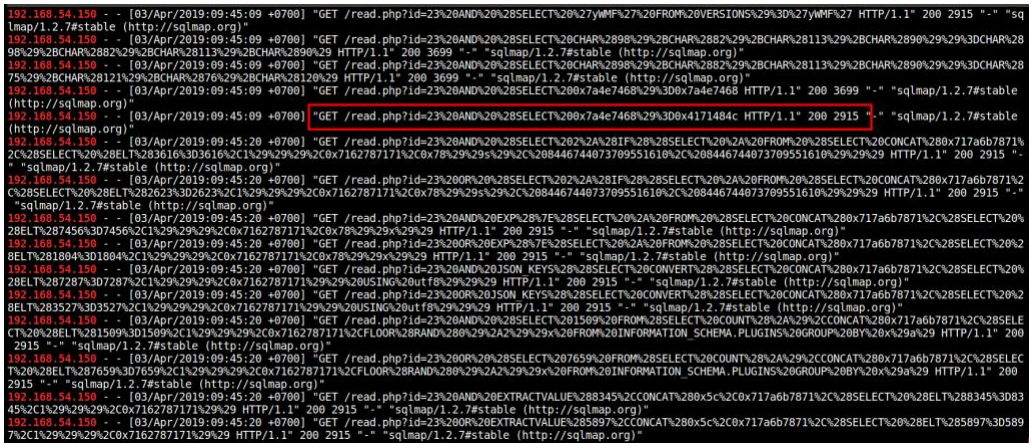
Gambar 11. Analisis *log* terkait *backdoor* b374k.php.

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 untuk mengetahui reputasi dari IP tersebut.



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.



Gambar 13. Analisis *log* lanjutan.

Selain itu juga terlihat penyerang melakukan serangan SQL dengan memasukan kode SQL pada salah satu halaman website. Didapatkan status code 200 pada setiap serangan SQL, dan dapat disimpulkan bahwa website mempunyai celah kerawanan pada serangan SQL.

6. Konfigurasi sudo

Ditemukan bahwa pada penyerang dapat melakukan privillege escalation dengan menggunakan kesalahan konfigurasi pada sudo dengan dibukanya akses aplikasi find dengan status NOPASSWD :

```
# sudo -l
```

Gambar 14. Temuan salah konfigurasi.

C. Containment

Untuk mengurangi dampak peningkatan resiko (mitigasi) perlu dilakukan hal-hal sebagai berikut :

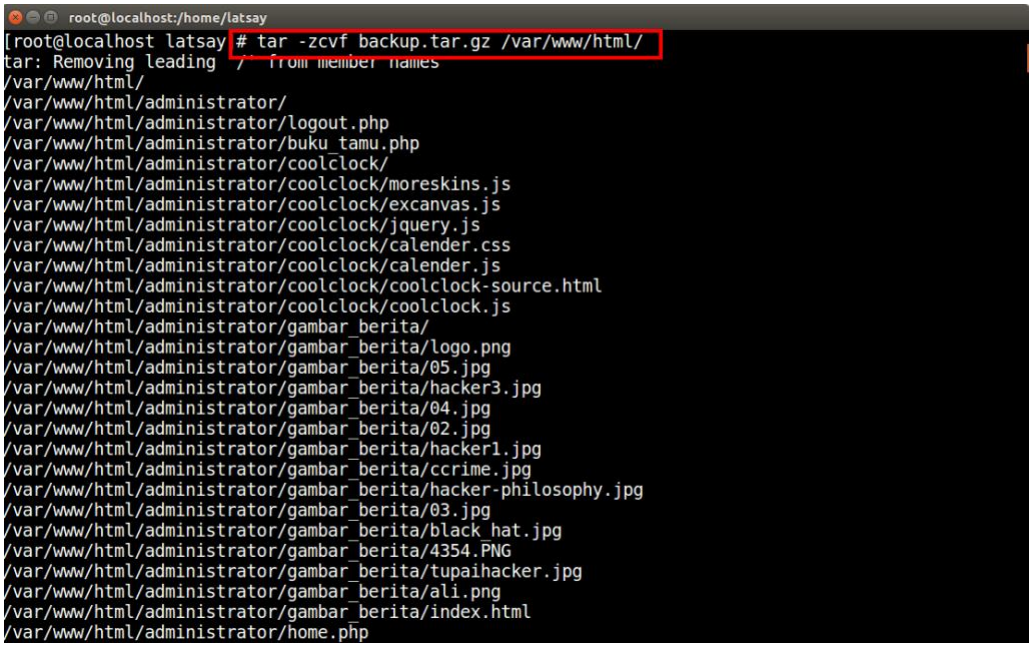
1. Lakukan backup system

Backup system dapat digunakan untuk mengumpulkan bukti-bukti insiden ataupun sebagai keperluan kegiatan Digital Forensic. Backup dilakukan pada direktori website yang terkena serangan ataupun backup pada seluruh sistem website.

a. Backup pada direktori

Backup pada direktori yang terkena insiden dilakukan dengan membuat file zip agar sumber serangan dapat disimpan dan menutup akses dari sumber serangan tersebut, contoh sintax yang dapat dilakukan adalah sebagai berikut :

```
# tar -zcvf archive-name.tar.gz directory-website
```
contoh :
```
# tar -zcvf backup.tar.gz /var/www/html/
```



Gambar 15. *Backup* pada *directory*.

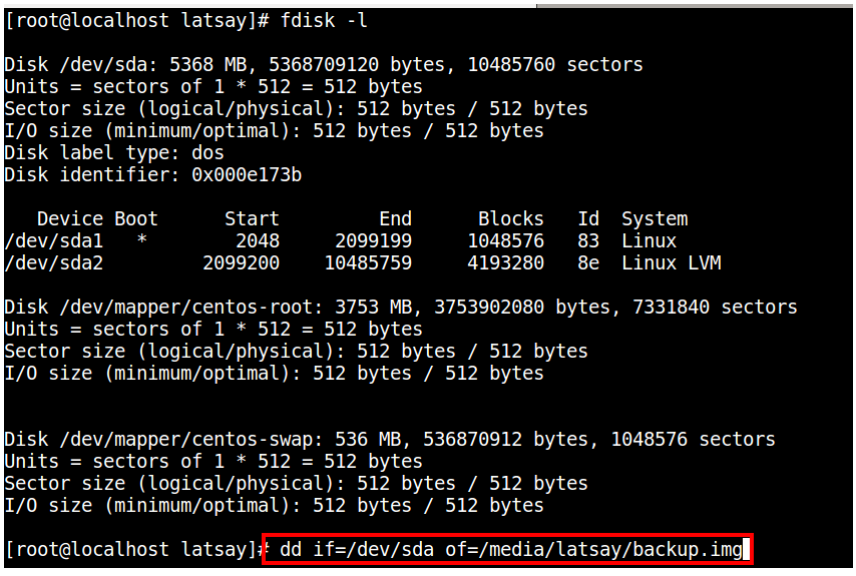
b. Backup seluruh sistem

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



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 berserta 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 ditunjukan dengan adanya status code 200 pada salah satu halaman website saat dilakukan serangan SQL.

2. Halaman administrator yang terlalu umum digunakan
Hal ini ditunjukan dengan mudahnya penyerang dalam mengakses halaman administrator.

3. Tidak menggunakan password yang sesuai dengan standar keamanan
Hal ini ditunjukan dengan mudahnya penyerang mendapatkan password yang digunakan oleh pengelola website.

4. Tidak adanya pembatasan pada file yang di-upload
Hal ini ditunjukan dengan diijinkannya file webshell yang diupload oleh penyerang.

5. Tidak adanya pembatasan pada file yang dapat diakses pada server
Hal ini ditunjukan dengan diijinkannya file webshell yang diupload dam diakses oleh penyerang.

6. Adanya misconfiguration dalam konfigurasi Visudo Hal ini ditunjukan 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