

L1 SOC ANALYST

Modul Praktikum 6

Menganalisis Dampak Insiden Keamanan Siber



J.62SOC00.018.1

MODUL PRAKTIKUM L1 SOC ANALYST

Unit Kompetensi

Menganalisis Dampak Insiden Keamanan Siber

Tujuan Praktikum

1. Menghilangkan bagian aset yang memiliki kerentanan
2. Mengetahui source code dari web yang menyebabkan kerentanan

Patching System (P.18.1.A)

Skenario Praktikum

Anda adalah seorang *L1 SOC Analyst* yang bekerja di Pemerintah Daerah Kabupaten Lengkeng. Anda memiliki tugas untuk mengawasi dan memantau seluruh aktivitas jaringan ke dalam infrastruktur TI Pemkab Lengkeng dengan bantuan SIEM. Sebelumnya anda telah mengenai kerentanan pada aset yang anda miliki dengan melakukan *vulnerability assesment* pada aset dan ditemukan bagian dari aset yang menimbulkan kerentanan yaitu vsftpd 2.3.4. Anda dimintai bantuan oleh administrator untuk memitigasi kerentanan ini. Anda tidak boleh menghilangkan vsftpd 2.3.4 dikarenakan masih digunakan oleh administrator.

Tujuan Praktikum

Praktikum ini bertujuan untuk membantu peserta didik dalam melakukan *patching* pada system

Environment Laboratorium Virtual

Praktikum ini membutuhkan:

- VM Kali Linux
- VM Target Web 1.

Durasi Praktikum

10 Menit

Catatan Khusus

- Siapkan *environment* laboratorium virtual sesuai panduan instalasi laboratorium virtual
- Dokumentasikan setiap langkah praktikum karena dapat membantu menjawab pertanyaan pada soal yang diberikan

Langkah-Langkah

1. Buka dokumentasi anda terkait praktikum modul 2 mengenai *vulnerabilty assesment*, jika anda melakukan dengan teliti praktikum 2 maka anda akan menemukan kerentanan pada vsftpd 2.3.4 yang ada dalam VM Target Web 1, seharusnya anda mengetahui bahwa vsftpf 2.3.4 terdapat *backdoor* didalamnya.
2. Lakukan SSH pada VM Target Web 1 melalui kali dengan memasukan perintah `ssh serveradmin@10.0.11`

```
(kali@kali) ~$ ssh serveradmin@10.0.1.11
serveradmin@10.0.1.11's password:
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-135-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

System information as of Wed Apr 30 03:45:56 AM UTC 2025

System load: 0.43556875          Processes: 133
Usage of /:  51.9% of 16.07GB    Users logged in: 0
Memory usage: 34%              IPv4 address for enp0s3: 10.0.1.11
Swap usage:  0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.
   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.
   https://ubuntu.com/pro
```

3. Cek versi VSFTPD yang digunakan dengan `vsftpd -version`. Dapat dilihat bahwa VSFTPD menggunakan versi yang *vulnerable* sesuai dengan hasil *vulnerability assessment*

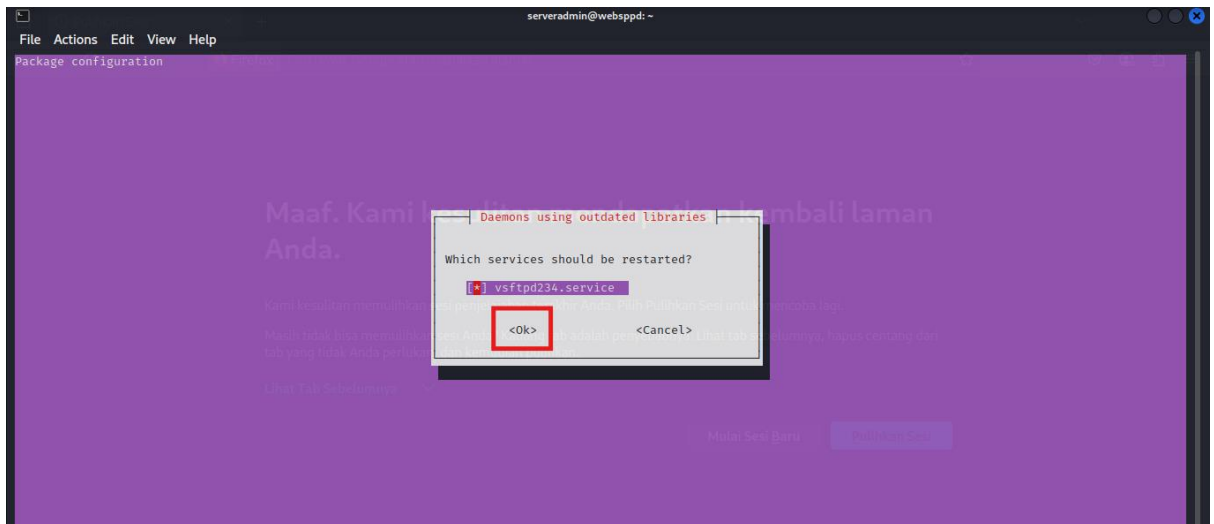
```
Last login: Fri Apr 11 07:08:00 2025 from 10.0.1.5
serveradmin@websppd:~$
serveradmin@websppd:~$
serveradmin@websppd:~$
serveradmin@websppd:~$
serveradmin@websppd:~$
serveradmin@websppd:~$
serveradmin@websppd:~$ vsftpd -version
vsftpd: version 2.3.4
```

4. Lakukan instalasi versi terbaru VSFTPD dengan perintah `sudo apt install vsftpd`, perintah ini akan otomatis melakukan instalasi versi terbaru dari vsftpd.

```
vsftpd: version 2.3.4
serveradmin@websppd:~$ sudo apt install vsftpd
[sudo] password for serveradmin:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 176 not upgraded.
Need to get 123 kB of archives.
After this operation, 326 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 vsftpd amd64 3.0.5-0ubuntu1.1 [123 kB]
Fetched 123 kB in 3s (44.5 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 122153 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.5-0ubuntu1.1_amd64.deb ...
Unpacking vsftpd (3.0.5-0ubuntu1.1) ...
Setting up vsftpd (3.0.5-0ubuntu1.1) ...

Configuration file '/etc/vsftpd.conf'
=> File on system created by you or by a script.
=> File also in package provided by package maintainer.
What would you like to do about it? Your options are:
  Y or I : install the package maintainer's version
```

5. Jika terdapat pilihan untuk service yang digunakan, pilih service yang telah ada sebelumnya, tidak masalah untuk nama service masih menggunakan vsftpd 2.3.4



6. Jika sudah selesai maka dapat dilakukan pengecekan versi dengan perintah yang sama yaitu `vsftpd -version`

```
serveradmin@websppd:~$ vsftpd -version
vsftpd: version 3.0.5
```

7. Jika skenarionya VSFTPD tidak lagi digunakan, anda dapat melakukan penghapusan layanan tersebut dengan `sudo apt purge vsftpd`
8. Jika anda hendak melakukan pembaharuan pada semua layanan yang ada anda dapat melakukan `sudo apt upgrade`

Mengenali source code web yang menyebabkan kerentanan (P.18.1.B)

Skenario Praktikum

Anda adalah seorang *L1 SOC Analyst* yang bekerja di Pemerintah Daerah Kabupaten Lengkeng. Anda memiliki tugas untuk mengawasi dan memantau seluruh aktivitas jaringan ke dalam infrastruktur TI Pemkab Lengkeng dengan bantuan SIEM. Sebelumnya anda telah mengenai kerentanan pada aset yang anda miliki dengan melakukan *vulnerability assesment* pada aset dan ditemukan bagian dari aset yang menimbulkan kerentanan yaitu kurangnya parameter kerentanan pada web sspd yang dihosting pada VM Web Target 1. Anda dimintai bantuan oleh administrator untuk mengenali bagian dari source code web sspd yang rentan dan saran perbaikannya.

Tujuan Praktikum

Praktikum ini bertujuan untuk membantu peserta didik dalam melakukan *patching* pada system

Enviroment Laboratorium Virtual

Praktikum ini membutuhkan:

- VM Kali Linux
- VM Target Web 1.

Durasi Praktikum

20 Menit

Catatan Khusus

- Siapkan *enviroment* laboratorium virtual sesuai panduan instalasi laboratorium virtual
- Dokumentasikan setiap langkah praktikum karena dapat membantu menjawab pertanyaan pada soal yang diberikan

Langkah-Langkah

1. Lakukan SSH pada VM Target Web 1 melalui kali dengan memasukan perintah `ssh serveradmin@10.0.11`

```
(kali@kali) ~$ ssh serveradmin@10.0.1.11
serveradmin@10.0.1.11's password:
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-135-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Wed Apr 30 03:45:56 AM UTC 2025

System load: 0.435546875   Processes:    133
Usage of /:  51.9% of 16.07GB   Users logged in: 0
Memory usage: 34%           IPv4 address for enp0s3: 10.0.1.11
Swap usage:  0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.
   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.
   https://ubuntu.com/pro
```

2. Buka direktori dimana *source code* web sppd disimpan, pada kasus ini terdapat pada `/var/www/sppd`. Anda dapat melakukan perpindahan direktori kerja anda dengab perintah `cd` sehingga `cd /var/www/sppd`. Lakukan perintah `ls` untuk mengecek isi direktori dimana anda berada.

```
* Management:  https://landscape.canonical.com
* Support:     https://ubuntu.com/advantage

System information as of Fri May  2 01:29:23 PM UTC 2025

System load: 0.1005859375   Processes:    125
Usage of /:  54.5% of 16.07GB   Users logged in: 0
Memory usage: 32%           IPv4 address for enp0s3: 10.0.1.11
Swap usage:  0%

 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.
   https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.
0 updates can be applied immediately.
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Mon Apr 28 03:03:14 2025
serveradmin@websppd:~$ cd /var/www/sppd
serveradmin@websppd:/var/www/sppd$ ls
bidun  components  db          index.php  kaid      login.php  node_modules  package.json  public  tailwind.config.js
boss   config      input.css  LICENSE    logout.php output.css  package-lock.json  README.md
```

3. Buka file `login.php` untuk mengecek apakah ditemukan bagian dari *source code* yang menimbulkan kerentanan. Masukan perintah `sudo nano login.php`. Masukan password '`ubuntu`' jika diminta untuk memasukan password.

```
System load: 0.1005859375   Processes:    125
Usage of /:  54.5% of 16.07GB   Users logged in: 0
Memory usage: 32%           IPv4 address for enp0s3: 10.0.1.11
Swap usage:  0%

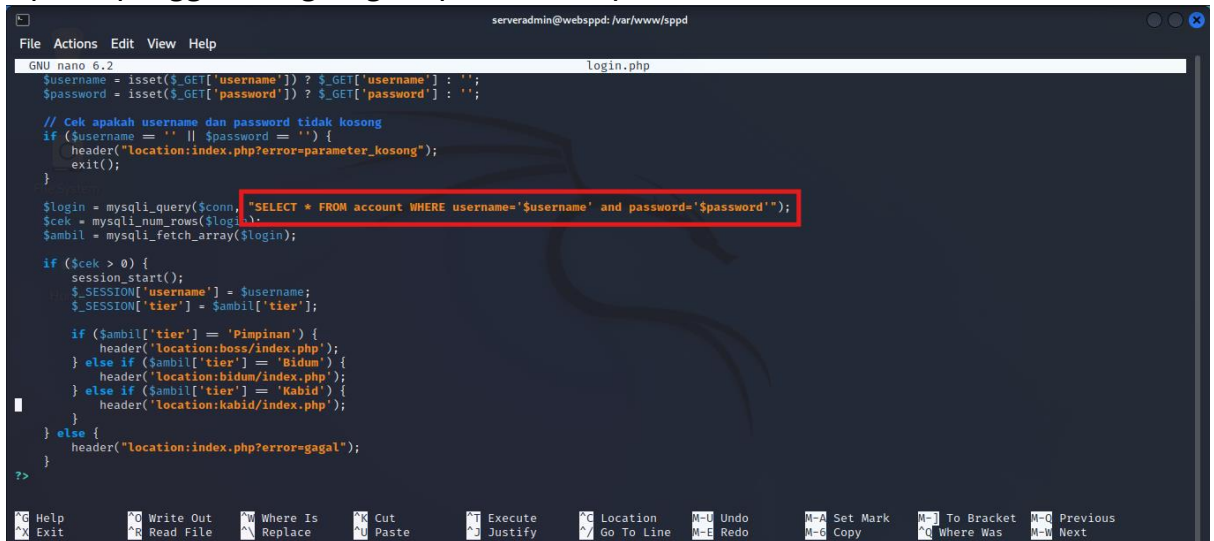
 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.
   https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.
0 updates can be applied immediately.
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Mon Apr 28 03:03:14 2025
serveradmin@websppd:~$ cd /var/www/sppd
serveradmin@websppd:/var/www/sppd$ ls
bidun  components  db          index.php  kaid      login.php  node_modules  package.json  public  tailwind.config.js
boss   config      input.css  LICENSE    logout.php output.css  package-lock.json  README.md
serveradmin@websppd:/var/www/sppd$ sudo nano login.php
[sudo] password for serveradmin:
```


4. Tampilan source code akan seperti berikut, lakukan analisis bagaimana kredensial pengguna diolah untuk login pada source code ini. Ditemukan keretanan dimana inputan pengguna langsung diinputkan ke SQL.



```
serveradmin@websppd: /var/www/lspdp
File Actions Edit View Help
GNU nano 6.2 login.php
$username = isset($_GET['username']) ? $_GET['username'] : '';
$password = isset($_GET['password']) ? $_GET['password'] : '';

// Cek apakah username dan password tidak kosong
if ($username == '' || $password == '') {
    header("location:index.php?error=parameter_kosong");
    exit();
}

$login = mysqli_query($conn, "SELECT * FROM account WHERE username='$username' and password='$password'");
$cek = mysqli_num_rows($login);
$sambil = mysqli_fetch_array($login);

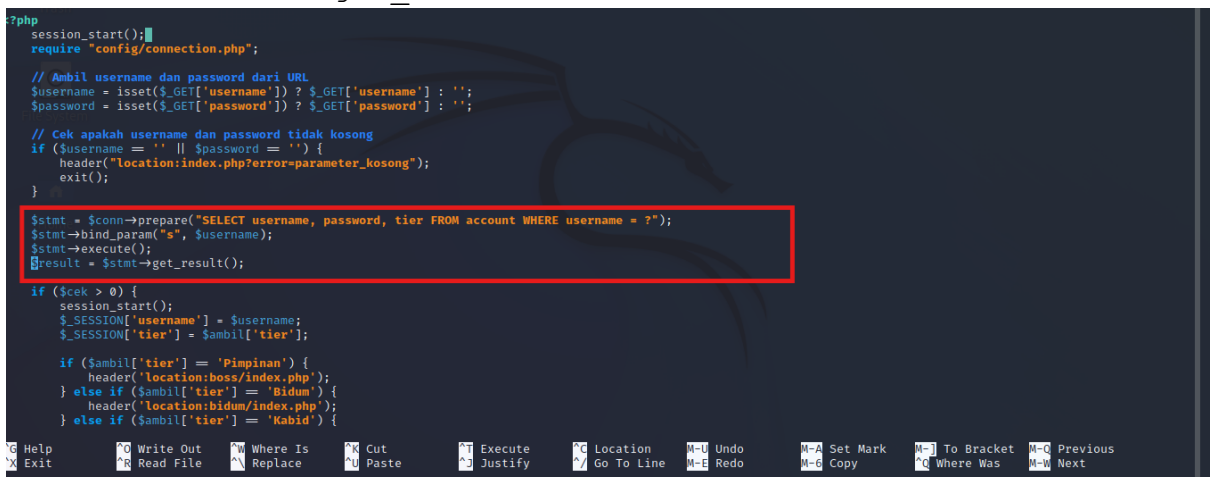
if ($cek > 0) {
    session_start();
    $_SESSION['username'] = $username;
    $_SESSION['tier'] = $sambil['tier'];

    if ($sambil['tier'] == 'Pimpinan') {
        header('location:boss/index.php');
    } else if ($sambil['tier'] == 'Bidum') {
        header('location:bidum/index.php');
    } else if ($sambil['tier'] == 'Kabid') {
        header('location:kabid/index.php');
    }
} else {
    header("location:index.php?error=gagal");
}

?>
```

5. Pada bagian tersebut lakukan *hardening* dengan mengganti source code dengan *prepared statement*

```
$stmt = $conn->prepare("SELECT * FROM account WHERE
username=? AND password=?");
$stmt->bind_param("ss", $username, $password);
$stmt->execute();
$result = $stmt->get_result();
```



```
?php
session_start();
require "config/connection.php";

// Ambil username dan password dari URL
$username = isset($_GET['username']) ? $_GET['username'] : '';
$password = isset($_GET['password']) ? $_GET['password'] : '';

// Cek apakah username dan password tidak kosong
if ($username == '' || $password == '') {
    header("location:index.php?error=parameter_kosong");
    exit();
}

$stmt = $conn->prepare("SELECT username, password, tier FROM account WHERE username = ?");
$stmt->bind_param("s", $username);
$stmt->execute();
$result = $stmt->get_result();

if ($cek > 0) {
    session_start();
    $_SESSION['username'] = $username;
    $_SESSION['tier'] = $sambil['tier'];

    if ($sambil['tier'] == 'Pimpinan') {
        header('location:boss/index.php');
    } else if ($sambil['tier'] == 'Bidum') {
        header('location:bidum/index.php');
    } else if ($sambil['tier'] == 'Kabid') {
        header('location:kabid/index.php');
    }
}

?>
```

6. Pada source code juga dapat kita cek bahwa tidak dilakukan *hashing* pada penyimpanan *password* karena tidak ditemukan fungsi untuk mengubah nilai hash dari inputan *password* pengguna. Contoh jika diimplementasikan dapat berupa `if (password_verify($password, $user['password'])) {`. Namun pada praktikum ini tidak akan dilakukan penambahan tersebut dikarenakan dari awal *password* yang disimpan dalam database tidak dilakukan *hashing*.
7. Untuk menyimpan perubahan tekan `ctrl+x` lalu `ctrl+y`.

