YOGYA EXECUTIVE SCHOOL
Jl. Gondang Raya No. 20 A Condongcatur Sleman Yogyakarta
Telp. 0274 737 1118 - Kode Pos 55283

Nomor : 0200744/YES/XI/2024
Lampiran : 3 lembar
Perihal : Pelatihan Penetration Testing

Yogyakarta, 28 November 2024

Kepada :
**Yth. Kepala Dinas Komunikasi dan Informatika**
**Kabupaten Penajam Paser Utara**
di Penajam

Dengan hormat,

Mengingat pentingnya upaya antisipasi terhadap tindakan serangan siber terhadap sistem keamanan server pemerintah daerah, pada kesempatan ini kami bermaksud mengundang **Dinas Komunikasi dan Informatika Kabupaten Penajam Paser Utara** untuk mengikuti **Pelatihan Penetration Testing** dengan ringkasan sebagai berikut:

a. Hari dan Tanggal : **Selasa s.d. Kamis, 3 – 5 Desember 2024**
b. Peserta : SDM aparatur Dinas Komunikasi dan Informatika Kabupaten Penajam Paser Utara yang berkompeten dan ditugaskan untuk mengikuti pelatihan ini.
c. Tempat : Gedung YES Jogja, Jl. Gondang Raya No. 20A Condongcatur Sleman D.I. Yogyakarta
d. Kontribusi : **Rp 5.000.000,00** (Lima Juta Rupiah) per peserta
e. Fasilitas :
- Tas, materi pelatihan, sertifikat, block note & alat tulis.
- Coffee break dan lunch.
- Kamar hotel selama 4 (empat) malam *include breakfast*.
- Antar jemput dari hotel ke tempat pelatihan.
- Antar jemput kedatangan dan kepulangan dari dan ke bandara, stasiun kereta atau terminal bus.

Demikian undangan pelatihan ini kami sampaikan dan atas perhatiannya mengucapkan terimakasih.

YOGYA EXECUTIVE SCHOOL

Wahyu Setiaji, SE
Direktur

Lampiran : 1 dari 3
Nomor : 0200744/YES/XI/2024
Tanggal : 28 November 2024

## LATAR BELAKANG

Penggunaan teknologi informasi pada penerapan Sistem Pemerintahan Berbasis Elektronik (SPBE) saat ini harus dijaga dan didukung oleh Information Security Policy. Ancaman keamanan informasi sangat nyata mulai dari kerusakan yang yang sederhana oleh virus/Trojan sampai penggunaan data informasi yang dapat diakses orang yang tidak berkepentingan dengan data tersebut. Pada umumnya celah security akan tidak tampak sebelum ada tindakan pengujian penetration.

Penetration testing, atau yang lebih dikenal dengan Pentest, adalah metode untuk menguji keamanan sistem jaringan komputer dengan cara melakukan simulasi serangan. Tujuannya adalah untuk menemukan celah keamanan yang bisa dimanfaatkan oleh pihak yang tidak berwenang. Dengan mengetahui celah keamanan tersebut, Diharapkan pengelola yang berwenang dapat mengambil langkah-langkah untuk memperbaikinya dan meningkatkan keamanan secara umum.

Peningkatan kualitas sumber daya manusia aparatur merupakan kunci keberhasilan organisasi dalam mencapai tujuannya. Hal ini perlu disadari, karena manusia merupakan subyek dan sekaligus obyek dalam pembangunan. Mengingat pentingnya menjaga keamaman sistem jaringan, oleh diperlukan dukungan ketersediaan SDM aparatur pengelola yang memiliki kompetensi yang memenuhi dalam pelaksanaan tugas. Hal ini dapat dicapai secara efektif melalui kegiatan pendidikan dan pelatihan, yaitu Pelatihan Penetration Testing (Pentest) bagi SDM Dinas Komunikasi dan Informatika Kabupaten Penajam Paser Utara yang berkepentingan dan/atau ditugaskan menjadi *Person in Charge* (PIC).

## DASAR HUKUM

1. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah;
2. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana diubah terakhir kali dengan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;
3. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik;
4. Peraturan Lembaga Administrasi Negara Nomor 10 Tahun 2018 tentang Pengembangan Kompetensi Pegawai Negeri Sipil.

## MAKSUD DAN TUJUAN

1. Maksud dari kegiatan pelatihan ini adalah sebagai upaya dalam rangka mewujudkan penerapan Sistem Pemerintahan Berbasis Elektronik (SPBE) di lingkungan Pemerintah Kabupaten Penajam Paser Utara dengan sistem keamanan yang baik.
2. Tujuan penyelenggaraan pelatihan adalah, diharapkan peserta:
   - Peserta dapat mengetahui kelemahan atau kerentanan system informasi yang terjadi server SPBE Dinas Komunikasi dan Informatika Kabupaten Penajam Paser Utara.
   - Peserta dapat lebih waspada untuk menjaga keamanaan informasi dikarenakan, peserta dapat melakukan proteksi dini sebelum ancaman pada keamnan itu terjadi.

Lampiran : 2 dari 3
Nomor : 0200744/YES/XI/2024
Tanggal : 28 November 2024

## METODE PELATIHAN

- Penyampaian teori melalui presentasi interaktif dengan proporsi 40 s.d. 50%
- Praktek komputer dan latihan dengan proporsi 50 s.d. 60%

## JUMLAH PESERTA

- Jumlah peserta minimal **10 (sepuluh)** orang.

## KETENTUAN LAIN

1. Konfirmasi kepastian keikutsertaan dengan menghubungi *contact person* kami.
2. Menjelang keberangkatan ke Yogyakarta pimpinan rombongan dimohon untuk mengkonfirmasikan jadwal kedatangan pada salah satu *contact person* kami.
3. Standar fasilitas kamar hotel adalah twin bed untuk 2 (dua) orang.
4. Biaya overtime hotel menjadi tanggung jawab peserta.
5. Pembayaran kontribusi dapat dilakukan secara tunai atau via transfer ke:
   - Nomor Rekening : 137-00-4333777-9
   - Atas Nama : CV. YOGYA EXECUTIVE SCHOOL "YES"
   - Bank : Bank Mandiri KCP Yogyakarta Katamso
6. Peserta berpakaian bebas, rapi, sopan dan bersepatu, atau sesuai arahan pimpinan.
7. Peserta membawa laptop, sudah menginstall **Virtual Box** dan **Kali Linux**.
8. Jika jadwal yang kami tawarkan tidak sesuai, dapat mengajukan permintaan jadwal khusus dengan memenuhi ketentuan jumlah peserta.

## CONTACT PERSON

- Enggar HP/WA : 0858 6786 5733
- Chandra HP/WA : 0852 2855 6902
- Dea HP/WA : 0812 2820 0303
- Nia HP/WA : 0822 4256 9068

Lampiran : 3 dari 3
Nomor : 0200744/YES/XI/2024
Tanggal : 28 November 2024

## JADWAL DAN MATERI

| Hari | Tanggal | Jam | Keterangan |
|---|---|---|---|
| Senin | 2 Des | 14:00 | Kedatangan peserta, penjemputan di bandara dan *check in* hotel |
| Selasa | 3 Des | 08:00 – 08:30 | Persiapan dan Pembukaan Pelatihan |
| | | 08:30 – 10:00 | Introduction to Security Assessment, Security Assessment, Vulnerability Assessment, Security Audit. |
| | | 10:00 – 10:30 | *Coffee break* |
| | | 10:30 – 12:00 | Penetration Testing, Vulnerability Assessment vs Penetration Testing, Penetration Testing vs Security Audit, Security Penetration Testing, Type Scope, Limitations. |
| | | 12:00 – 13:00 | Ishoma |
| | | 13:00 – 15:00 | Penetration Testing Standard and Methodology, Information Gathering Network Mapping, Vulnerability Identification, Gaining Access, Enumerating Compromising Remote Users, Maintaining Access, Covering Tracks. |
| | | 15:00 – 15:30 | Kembali ke hotel |
| Rabu | 4 Des | 08:00 – 08:30 | Persiapan pelatihan |
| | | 08:30 – 10:00 | Practice on VA tools usage. |
| | | 10:00 – 10:30 | *Coffee break* |
| | | 10:30 – 12:00 | whois, backlink checker |
| | | 12:00 – 13:00 | Ishoma |
| | | 13:00 – 15:00 | Google Dorking |
| | | 15:00 – 15:30 | Kembali ke hotel |
| Kamis | 5 Des | 08:00 – 08:30 | Persiapan pelatihan |
| | | 08:30 – 10:00 | Practice on Pentest tools usage. |
| | | 10:00 – 10:30 | *Coffee break* |
| | | 10:30 – 12:00 | NMAP, ZAProxy, SQL Injection & XSS on DVWA. |
| | | 12:00 – 13:00 | Ishoma |
| | | 13:00 – 15:00 | Make a Report of Penetration Testing |
| | | 15:00 – 15:30 | Penutupan/penyelesaian administrasi |
| Jumat | 6 Des | 12:00 | *Check out* hotel dan pengantaran kepulangan peserta ke bandara. |