Deep Offensive Hacking (Custom Workshop)

Objektif Pelatihan:

- Mensimulasikan aktivitas serangan untuk mengevaluasi keamanan yang terdapat pada sistem (tanpa Automation Scanner) sesuai dengan salah satu BoK badan sertifikasi ternama.

Metode Pelatihan:

- Hands-on Lab (Disampaikan dengan sekitar 7 lab berbeda dalam waktu sekitar 6 jam)

Silabus Pelatihan:

Jam Pertama (2 Labs):

1. **General - Additional.**
1.1. Introduction to Linux
1.2. Basic Command of Linux
1.3. Basic IP Calculation
1.4. Setting up Pentesting Environment

2. **General - Information Gathering.**
2.1. Active vs Passive
2.2. Operating System Identification
2.3. Ports / Services Identification
2.4. Services Enumeration

3. **Vulnerability Identification.**
3.1. ~~Dealing with Vulnerability Scanning Tools~~
3.2. Identifying the Vulnerability and Analyzing the Problem

4. **System Hacking – Exploiting – Part I**
4.1. Overview of Common Services
4.2. Having Fun with 3rd Party Services
4.3. Working with Web Shell
4.4. Context of Privilege Escalation
4.5. Password Cracking
4.5.1. Type of Brute Force Attack
4.5.2. Having Fun with Dumping Process

Jam ke-2 (1 Lab):

5. **System Hacking – Exploiting – Part II**
5.1. Information Gathering and Vulnerability Identification
5.2. Working with Public Exploit
5.3. Password Cracking
5.4. Context of Privilege Escalation
5.5. Local versus Remote Exploit

Jam ke-3 sampai sekitar Jam ke-5 (2 Labs):

6. **System Hacking – Exploiting – Part III**
6.1. Information Gathering and Vulnerability Identification
6.2. Working with Public Exploit
6.3. Context of Privilege Escalation

Jam ke-5 sampai sekitar Jam ke-6 (2 Labs):

7. **System Hacking – Exploiting – Part III**
7.1. Buffer Overflow Overview
7.2. Fuzzing Process
7.3. Buffer Overflow with Debugging Tool
7.4. Working with own Exploit
7.4.1. Shellcode Overview
7.4.2. Bad Character Overview
7.5. Bind versus Reverse Connection
7.6. Simple Challenge (Combining all of the topic)

Kebutuhan Pelatihan:

- **Peserta**: Perangkat Lunak **VMWare Workstation** (> v.12) / **VMWare Fusion** (> v.8) – Dapat menggunakan versi trial selama 30 hari:
    - http://www.vmware.com/products/workstation.html
    - http://www.vmware.com/products/fusion.html
- **Peserta**: Sistem operasi Kali Linux OS yang dapat diletakan pada VMWare ataupun menjadi Main Machine:
    - https://images.offensive-security.com/virtual-images/Kali-Linux-2016.2-vm-amd64.7z (64 bit VMWare Image);
    - https://images.offensive-security.com/virtual-images/Kali-Linux-2016.2-vm-i686.7z (32 bit VMWare Image)
    - http://cdimage.kali.org/kali-2016.2/kali-linux-2016.2-amd64.iso (64 bit ISO);
    - http://cdimage.kali.org/kali-2016.2/kali-linux-2016.2-i386.iso (32 bit ISO).
- **Dukungan**: 2 (dua) Notebook tambahan yang dapat digunakan sebagai target (akan diletakan Lab VM di dalam notebook ini – dengan asumsi jumlah peserta sekitar 30 peserta);
    - Masing-Masing notebook ter-install sistem operasi 64 bit (lebih baik bila Microsoft Windows OS) dengan minimal RAM sebesar 4 GB;
    - Masing-Masing sistem operasi telah memiliki VMWare Workstation terbaru (dapat versi trial yang diunduh pada portal resminya).
- **Dukungan**: Koneksi jaringan yang tidak dibatasi untuk para peserta sehingga dapat berkomunikasi satu sama lain, sebagai contoh melakukan ping ataupun menarik data.