Skill Exam Computer Security

Nama:

Periode:

Perkenalan:

Dalam penilain keterampilan ini, anda akan mencoba untuk melakukan “deployment”, “configuration” dan “security testing” di sebuah server “production”. Anda akan mendapatkan tugas untuk melakukan konfigurasi server, instalasi server dan evaluasi keamanan server. Untuk melakukan ujian ini anda dianggap sudah mempunyai virtual box yang sudah terinstall Kali Linux dan server Ubuntu 20.04 LTS.

Jika belum mempunyai Kali Linux anda dapat mendownload dan mengimport dari https://www.kali.org/get-kali/#kali-virtual-machines pilih yang ada logo virtual box. Lalu untuk Ubuntu 20.04 LTS sendiri anda dapat mencoba untuk menginstall sendiri lewat .iso yang bisa di download di ubuntu-20.04.6-live-server-amd64.iso atau anda bisa mendownload versi virtualbox di **ubuntu-osboxes.iso,** anda diberi kebebasan untuk memilih dari kedua versi yang sudah disediakan.

Anda akan berlatih dan dinilai berdasarkan keterampilan berikut:

- Konfigurasi pengaturan perangkat awal
- Instalasi dan konfigurasi server
- Kejelasan dalam penulisan penjelasan langkah-langkah dalam menyelesaikan tugas yang diberikan
- Kreatifitas dalam eksekusi exploitasi celah keamanan
- Kreatifitas dalam mencari lubang keamanan

Hasil dari ujian praktek ini adalah sebuah laporan yang menjelaskan bagaimana menyelesaikan tantangan dari setiap sesi yang diberikan Tidak ada format laporan yang harus diikuti oleh peserta yang terpenting adalah laporan rapih dan mudah dibaca. Di akhir ujian ini perserta akan mengerti bagaimana caranya membangun dan menyerang server secara detail.

Sesi 1 – Konfigurasi - 10 Poin

Di sesi ini peserta diekspektasi dapat melakukan konfigurasi ip address statik dalam mesin kali linux dan ubuntu VM, berikut adalah detail konfigurasi yang harus diikuti:

Nama mesin: kali linux
IP Address: 192.168.100.10/24
Gateway: 192.168.100.1

Nama mesin: ubuntu

IP Address: 192.168.100.20/24
Gateway: 192.168.100.1

Jika kedua konfigurasi sudah di implementasi, murid harus menjelaskan bagaimana cara melakukan konfigurasi ip secara detail di laporan dan pastikan kedua mesin vm dapat melakukan kontak satu sama lain, peserta dapat membuktikan dengan menaruh screenshoot kedua mesin mengirimkan “ping” satu sama lain.

Sesi 2 – Deployment - 40 Poin

Di sesi ini akan dibagi menjadi 4 bagian yang memiliki poin yang berbeda-beda:

Sesi 2.1 – 10 poin

Lakukan instalasi openssh dan mysql server di server ubuntu. Setelah openssh dan mysql server terinstall, peserta harus mengubah port openssh yang awalnya dari port 22 menjadi port 22888 dan port mysql yang awalnya 3306 menjadi 3390.

Jika konfigurasi sudah di implementasi murid harus menjelaskan bagaimana cara melakukan konfigurasi server ssh dan mysql secara detail di laporan. Pastikan peserta menyertakan screenshoot yang membuktikan bahwa openssh dan mysql server berjalan dengan baik dengan cara melakukan login ssh dan mysql dari kali linux ke ubuntu server.

Sesi 2.2 – 10 poin

Lakukan instalasi apache server dan php 8 di server ubuntu. Setelah apache server dan php 8 sudah terinstall murid harus menjelaskan bagaimana cara melakukan instalasi kedua komponen tersebut secara detail di laporan. Pastikan peserta menyertakan screenshoot yang membuktikan bahwa apache server berjalan dengan baik dengan cara melakukan mengujungi web server dari kali linux ke ubuntu server dengan memakai web browser dari kali linux.

Sesi 2.3 – 20 poin

Lakukan deployment Webutler v3.2 di dalam apache server, source code tersebut dapat di download dari http://webutler.de/download/webutler_v3.2.zip, peserta dapat mengikuti cara deployment dari https://webutler.de/en. Setelah Webutler v3.2 sudah terinstall peserta harus menjelaskan bagaimana cara melakukan deployment secara detail di laporan. Pastikan peserta menyertakan screenshoot yang membuktikan bahwa Webutler v3.2 berjalan dengan baik dengan cara melakukan mengujungi aplikasi dari kali linux ke ubuntu server dengan memakai web browser dari kali linux.

Sesi 3 – Security Testing - 50 Poin

Di sesi ini akan dibagi menjadi 3 bagian yang memiliki poin yang berbeda-beda:

Sesi 3.1 – 10 poin

Lakukan port scanning memakai nmap dari kali linux ke ubuntu server pastikan dalam hasil scanning tercantum port server yang sudah terinstall di sesi sebelumnya dan versi service yang berjalan di masing-masing port yang ditemukan. Setelah port scanning sudah dilakukan peserta harus menjelaskan bagaimana cara melakukan teknik tersebut secara detail di laporan, pastikan hasil scanning tercantum port server yang terbuka dan service yang berjalan di masing-masing port.

Sesi 3.2 – 10 poin

Setelah melakukan port scanning lakukan eksploitasi ke server ssh dan mysql dengan memakai modul Metasploit di kali linux:

- auxiliary/scanner/ssh/ssh_login
- auxiliary/scanner/mysql/mysql_login

Jelaskan cara kerja dan cara memakai masing-masing modul dalam laporan dan berikan hasil yang diberikan dan jelaskan kenapa bisa memberikan hasil tersebut.

Sesi 3.3 – 30 poin

Lakukan eksploitasi ke webutler v3.2 dari kali linux, peserta diberikan kebebasan untuk bagaimana mengeksekusi exploitasi nya sampai mendapatkan RCE (Remote Code Execution) ke ubuntu server. Pastikan untuk mencatat semua proses eksploitasi sampai selesai di laporan: https://www.exploit-db.com/exploits/51660