SKENARIO

ETHICAL HACKING AND PENETRATION TESTING I

Dosen Pengampuh : Runal Rezkiawan S,Kom., M.T

DI SUSUN OLEH

NAMA : NUR ALIYAH AMALIANI

NIM : 105841106923

KELAS : 5 JK-B

PROGRAM STUDI INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH MAKASSAR

2025

SKENARIO DAN TAHAPAN TEKNIS

Dalam simulasi ini, saya berperan sebagai Konsultan Keamanan Siber. Tugas utama saya adalah melakukan audit (pemeriksaan) keamanan untuk mencari tahu apakah ada celah atau kelemahan pada sistem target.

Metode yang saya gunakan adalah Black-Box Testing. Artinya, saya memposisikan diri sebagai penguji dari pihak luar yang tidak memiliki akses login atau bocoran informasi apa pun tentang sistem target. Tujuannya adalah untuk mensimulasikan bagaimana seorang peretas (hacker) sungguhan mengumpulkan informasi dan mencari jalan masuk.

Pemeriksaan dibagi menjadi dua target operasi:

1. Target Eksternal (Tokopedia). Ini fokus pada pengumpulan data publik (Passive Recon) untuk memetakan permukaan serangan tanpa interaksi ilegal
2. Target Internal (VulnOS). Ini fokus pada pemindaian jaringan (Active Recon) dalam lingkungan terisolasi untuk menemukan kerentanan teknis

Berikut adalah langkah-langkah pengerjaan yang dilakukan secara berurutan:

A. TAHAP 1: PERSIAPAN LAB

Tahap ini bertujuan membangun lingkungan kerja yang aman dan memastikan alat siap digunakan.

1. Instalasi Laboratorium
    - Menyiapkan Oracle VirtualBox sebagai hypervisor
    - Mendownload, Install, dan mengimport mesin virtual VulnOS v2 sebagai target.
    - Mendownload dan menginstall Nmap
    - Mendownload dan menginstall Wireshark untuk sampel network traffic
2. Konfigurasi jaringan
    - Mengubah pengaturan Network Adapter pada VulnOS menjadi Host-only Adapter. Tujuannya untuk menciptakan jaringan privat antara

laptop (Host) dan VulnOS (Guest) agar proses scanning tidak bocor ke jaringan publik/internet

B. TAHAP 2 PASSIVE RECONNAISSANCE (TARGET TOKOPEDIA)

Tahap ini dilakukan sepenuhnya menggunakan koneksi internet publik tanpa menyentuh server target. Serta menggunakan wifi pribadi.

1. Pencarian Sub-Domain (Enumerasi)
   - Pada tahap ini saya menggunakan teknik Google Dorking pada mesin pencarian google.
   - Dengan mengetikkan perintah *site:tokopedia.com -www* di kolom pencarian. Ini bertujuan untuk memfilter dan membuat halaman (www), sehingga halaman-halaman yang tersembunyi atau portal khusus seperti accounts (halaman login) dan seller (halaman penjual) bisa muncul
2. Pencarian Informasi karyawan dan Email
   - Pada tahap ini saya melakukan riset profil profesional menggunakan situs LinkedIn dan Hunter.io
   - Disini saya menggunakan 2 perintah, yang pertama *site:id.linkedin.com/in/ "Tokopedia" AND ("Security" OR "Head"),* perintah ini untuk mencari pejabat penting pada target. Kedua *Tokopedia" email format hunter.io* perinta ini untuk mencari pola email karyawan perusahaan target. Perintah ini dijalankan di google dengan teknik google dorking
3. Pencarian teknologi apasaja yang digunakan

   Tahap selanjutnya setelah mencari data karyawan target, kita akan menganalisis situs target menggunakan alat pemindai teknologi bernama BuiltWith. Dimana pada tahap ini kita memasukkan alamat domain tokopedia.com kedalam situs builtwith.com tersebut. Maka akan muncul semua informasi terkait teknologi apa saja yang digunakan oleh target. Komponen yang perlu diperhatikan di pencarian teknologi target ini yaitu Web server, Content Deliveri Network (CDN), dan Library javascript
4. Pencarian informasi sensitif yang bocor atau terekspos di publik

Setelah mencari informasi mengenai teknologi yang digunakan oleh target, langkah selanjutnya adalah mencoba mencari informasi sensitif yang bocor ke publik. Langkah pertama yang dilakukan adalah mencari file bocor menggunakan teknik google dorking dengan memasukkan perintah *site:tokopedia.com filetype:pdf "confidential"* dan *site:tokopedia.com filetype:docx.* Atau perintah *site:tokopedia.com filetype:pdf.* perintah perintah ini digunakan untuk menampilkan semua file pdf dengan kata kunci confidential, atau file docx, atau file pdf tanpa kata kunci spesifik.

selanjutnya cari juga informasi bocor di github, pertama login ke github kemudian dibagian pencarian ketik *"tokopedia.com" filename:config*, kode ini untuk mencari fil konfigurasi yang menyebut nama tokopedia. Kemudian setelah memasukkan perintah *"tokopedia.com" filename:config* masukkan lagi perintah *api.tokopedia.com* untuk menembak langsung ke API server mereka.

C. TAHAP 3 ACTIVE RECONNAISSANCE (TARGET VULNOS

Tahap ini dilakukan di jaringan lokal (Host-only) terhadap IP Target 192.168.56.20

1. Mengaktifkan target

   Sebelum memindai target. Target harus aktif dan terhubung. Langkah yang paling dari dari tahap ini adalah mendownload vunlOS melalui link berikut VulnOS: 2 ~ VulnHub kemudian extrak dan install. Setelah install, masuk ke virtual box, kemudian klik open kemudian pilih file dengan extention vbox. Kemudian open. Setelah itu jangan langsung masuk. Tapi setting jaringannya terlebih dahulu. Masuk kebagian setting, kemudian pilih network, pilih adapter 1 setelah itu pada bagian Attached to pilih Host-only Adapter, kemudian Promiscuous Mode pilih Allow All. Setelah di setting klik oke kemudian jalan kan VulnOS. Setelah masuk di VulnOS maka akan meminta username dan password masukkan root untuk masing masing username dan password. Kemudian jalankan perinta ip a untuk melihat ip address target

2. Pengecekan Konektivitas

   Setelah mengaktifkan target. Masuk kebagian CMD kemudian ping ip address target. Jika suda terbaca TTL maka target sudah dipastikan aktif.

3. Validasi Trafik jaringan

   Setelah yakin target aktif langkah selanjutnya adalah validasi trafik. Sebelum itu download dan install terlebih dahulu wireshak. Setelah berhasil di install, klik dua kali untuk masuk. Setelah masuk, pilih interface yang aktif. Pilih adapter virtualBox Host-Only di wireshark lihat di CMD virtualBox memakai ethernet berapa. Dengan perintah ip config. Setelah tau dan memilih interface VirtualBox saatnya klik interfacenya kemudian klik sirip biru untuk memulai capture.

4. Pemindaian Port terbuka

   Setelah memulai caputer di wireshark, sekranga kita akan memindai port yang terbuka. Caranya buka kembali CMD di windows kemudian jalankan perintah *nmap -sS -sV -0 192.168.56.20,* perintah ini digunakan untuk melakukan pemindaian diam diam. Ini menggunakan parameter -sS (TCP SYN Scan). Setelah menjalankan perintah akan terlihat port apa saja yang terbuka.

5. Pemindaian Port UDP

   Selanjutnya melakukan pemindaian khusus untuk prpotokol UDP karena protokol ini berbeda dengan TCP. Perintahnya *nmap -sU --top-ports 20 192.168.56.20* jika perintah ini dijalankan maka akan memeriksa 20 layanan UPD terpopuler (seperti DNS atau SNMP) untuk memastikan tidak ada celah yang terlewat di protokol ini. Hasilnya nanti akan terlihat, jika port udp nya terbuka maka akan ada tanda open. Tapi jika semua nya tertutup maka akan ada keterangan close.

6. Pemindaian untuk mendeteksi layanan (service) dan versi perangkat lunak, yang berjalan pada port port tersebut.

   Setelah melakukan melakukan scan port yang terbuka, selanjutnya disini kita meminta Nmap untuk memberikan informasi dan membocorkan

nama aplikasi yang digunakan target. Dengan menggunakan perintah -sV (Version Detection), maka nanti akan muncul versi software yang dipakai.

7. Mengidentifikasi sistem operasi (OS) yang digunakan oleh target

   Selanjutnya di bagian perintah terakhir tambahkan parameter -O (OS Detection). Ini digunakan untuk menganalisis paket jaringan untuk menebah jenis sistem operasi target.