CYBER KILL CHAIN METHODOLOGY

Pemateri

Ust Aiman Alauddin Fadhullah Al-Fatih

Disusun Oleh :

Fahmi Ramadan

Pondok Pesantren Siber Bandung

Bumi sariwangi 2, Blk. B, Sariwangi, Parongpong, West Bandung Regency, West Java 40559

1. Apa itu *Cyber Kill Chain Methodology*

Cyber Kill Chain, ditemukan oleh Lockheed Martin, merupakan runtutan beberapa fase serangan siber. Tiap serangan merepresentasikan sebuah kesempatan untuk mendeteksi dan mereaksi terhadap sebuah serangan.

Pada istilah militer "*kill chain*" adalah model yang berbasis fase untuk mendeskripsikan tahapan dalam sebuah serangan, yang juga memberi informasi bagaimana cara untuk mencegah serangan tersebut.

Semakin cepat *kill chain* dapat dihentikan, semakin sedikit pula informasi yang dimiliki oleh peretas, semakin sedikit kemungkinan orang lain dapat menggunakan informasi tersebut untuk melengkapi serangannya nanti.

Cyber Kill Chain merupakan sebuah framework yang dimana memposisikan diri sebagai penyerang untuk mengetahui kekurangan dari suatu situs/sistem. Dengan framework ini team Security Auditing mempermudah melakukan pencarian kekurangan dari objek. *Cyber Kill Chain* ini memiliki 7 tahapan diantaranya; *Reconnaissance*, *Weaponize*, *Delivery*, *Exploitation*, *Installation*, *Command Control (C2)*, *Act on Objective*. Sehingga akan didapatkan klasifikasi berupa hubungan antara tools dan vulnerability berdasarkan framework Cyber Kill Chain.

Cyber Kill Chain yang ditemukan oleh Lockheed Martin, yang mendeskripsikan serangan secara terstruktur, bekerja seperti sebaliknya, dapat digunakan sebagai pengamanan untuk jaringan organisasi. Langkah langkahnya didapati dibawah ini :

1.1. Reconnaissance

Reconnaissance adalah tahap mengumpulkan data, dimana hacker akan mengumpulkan data tentang target sebanyak-banyaknya. Baik nama anggota keluarga, tanggal lahir, tempat kerja beserta informasi didalamnya. Pada fase ini, peretas mencoba untuk menentukan target yang dirasa bernilai. Mereka menilai apakah target tersebut sepadan.

- *Passive Reconnaissance*: Langkah ini dilakukan dengan mengumpulkan informasi tentang target tanpa memberitahukannya.
- *Active Reconnaissance*: Langkah ini melibatkan profil target yang jauh lebih dalam yang mungkin memicu peringatan ke target.

1.2. Weaponization

Tergantung dari jumlah dan kualitas informasi yang berhasil didapatkan dari proses reconnaissance, attacker akan mulai menyusun skenario serangan yang paling cocok terhadap targetnya, dan tahap ini disebut weaponization. Tahapan ini lebih banyak terjadi pada sisi attacker sehingga cukup sulit dideteksi sampai serangan tersebut dijalankan.

Fase ini sangat bergantung pada informasi hasil reconnaissance sehingga untuk mengurangi tingkat keberhasilan dari attacker dapat dilakukan pembatasan informasi apa saja yang mungkin dapat diketahui oleh attacker pada fase reconnaissance. Dan juga memastikan bahwa setiap vulnerability yang terdapat pada jaringan internal dilakukan patch sebelum berhasil dieksploitasi oleh attacker.

1.3. Delivery

Skenario yang telah disiapkan sebelumnya pada fase weaponization kemudian dijalankan pada fase delivery. Payload ataupun exploit yang telah dipilih

sebelumnya akan dikemas sedemikian hingga dan dikirmkan ke target dengan berbagai cara misal saja seperti lewat email, usb flash-drive yang sengaja dijatuhkan didekat lokasi target, atau melalui website yang telah disusupi payload dan mengarahkan target untuk mengunjungi website tersebut. Berbagai teknik delivery ini akan tergantung dari jenis informasi apa yang didapat pada fase reconnaissance dan skenario serangannya. Attacker yang berpengalaman biasanya memiliki lebih dari 1 skenario untuk mengantisipasi jika skenario yang lain gagal.

1.4.Exploit

Exploitation adalah tahapan selanjutnya setelah exploit atau payload berhasil dikirimkan, diterima dan dijalankan oleh target. Exploit akan dijalankan dan mengeksploitasi vulnerability yang ada pada target menyebabkan perangkatnya ter-compromise. Exploitini bisa diberikan langsung pada tahap delivery ataupun hanya berupa dropper dimana exploit yang sesungguhnya akan didownload dari internet saat dropper tersebut dijalankan oleh target.

1.5. Installation

Peretas memasang malware pada sistem target. Instalasi dari Remote Access Trojan (RAT) dan backdoor pada target membuat attackermemiliki akses berkelanjutan pada sistem target untuk melancarkan serangan lanjutan ataupun mengincar target lainnya. Attacker yang terlatih dan berpengalaman akan dengan mudah menyembunyikan RAT dan backdoor yang diinstallnya untuk menghindari deteksi, RAT dan backdoor jenis ini biasanya merupakan varian yang telah dimodifikasi.

Sistem deteksi tingkat lanjut dapat diimplementasikan untuk memitigasi serangan pada tahap ini. Salah satu contoh implementasi yang biasa dilakukan adalah dengan melakukan monitoring pada event logs dan registry sistem. Berbagai macam perubahan pada sistem akan dideteksi oleh sistem monitoring. Application whitelisting juga bisa dipakai untuk mencegah RAT dan backdoor dapat diinstall pada system.

1.6. Command and Control

Peretas membuat channel untuk mengontrol sistem tersebut secara remote. Command and Control (C2) dipakai oleh attacker untuk mengontrol sistem target yang telah ter-compromise secara penuh. C2 ini bisa diimplementasikan pada berbagai protokol tergantung dari kemampuan attacker, C2 yang umum adalah via protokol yang tidak terenkripsi seperti HTTP, DNS, ICMP, dan IRC. Beberapa attacker yang terlatih akan memakai jalur komunikasi terenkripsi untuk menghindari pendeteksian seperti HTTPS dan SSH.

1.7. Actions

Setiap attacker pasti memiliki tujuan saat melancarkan serangannya, entah itu hanya untuk melatih kemampuan dan untuk pamer atau yang lebih serius lagi seperti pencurian informasi dan cyberterrorism. Ketika attacker telah berhasil mencapai targetnya maka security analyst yang melakukan NSM dan CSM sebagai defender dapat dikatakan gagal dalam menjalankan tugasnya. Oleh karena itu salah

satu tugas security analyst adalah untuk mencegah attacker mendapatkan tujuannya, medeteksi serangannya dan memutus serangan tersebut pada fase atau tahap yang tepat sesuai Intrusion Kill Chain.

2. **Contoh *Cyber Kill ChainMethodology***

SKENARIO : Attacker ingin mengetahui foto-foto yang tersimpan HP di gallery mantannya

2.1. Recconassance

Penyerang memulai mengumpulakn informasi dari korban, baik lewat social medianya (*passive*) atau melakukan rekayasa social (*active*) untuk mengetahui jenis atau spesifikasi handpone. Ternyata di Instagram korban terlihat dari fitur 'Add yours' bahwa handphonenya bertipe android merk X.

2.2. Weaponization

Oke udah tau nih hpnya jenis X, sekarang kita buat backdoor/malware untuk disisipkan ke handphonenya. Dan disini penyerang membuat sebuah backdoor apk game (mis. Game bounch)

2.3. Delivery

Terus gimana ya biar mantannya mengintall apk ini?. Disini dibutuhkan Teknik social engineering. Kebetulan pada suatu hari terdapat pertemuan reuni SMA. Penyerang ini membuat scenario acara supaya mantannya menginstall apk ini.

2.4. Exploitation

Pada tahap ini payload sudah berhasil dikirimkan di HP mantan.

2.5. Installation

Oke aplikasi sudah terpasang. Lalu pada tahap ini juga dilakukan monitoring log dan registry sistemnya. Sehingga kita bisa melanjutkan ke tahap berikutnya.

2.6. Command and Control

C2 fase ini attacker mengontrol sistemnya lewat jalur komunikasi yang tidak terenkripsi. Biasanya attacker menghindari HTTPS dan SSH. Disini penyerang sudah bisa memberikan command untuk meremorte HP mantannya.

2.7. Actions on Objectives

Pada fase ini penyerang sudah bisa melihat foto-foto di gallery manntanya. Eitss tapi ternyata si mantan memakai password untuk membuka gallerya (terenkripsi). Jadi penyerang ngga bisa deh buka foto-foto yang ada di gallery mantannya.

SUMBER :

https://kuebasi.wordpress.com/2018/07/08/tugas-5-kill-chain-rat/

https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html