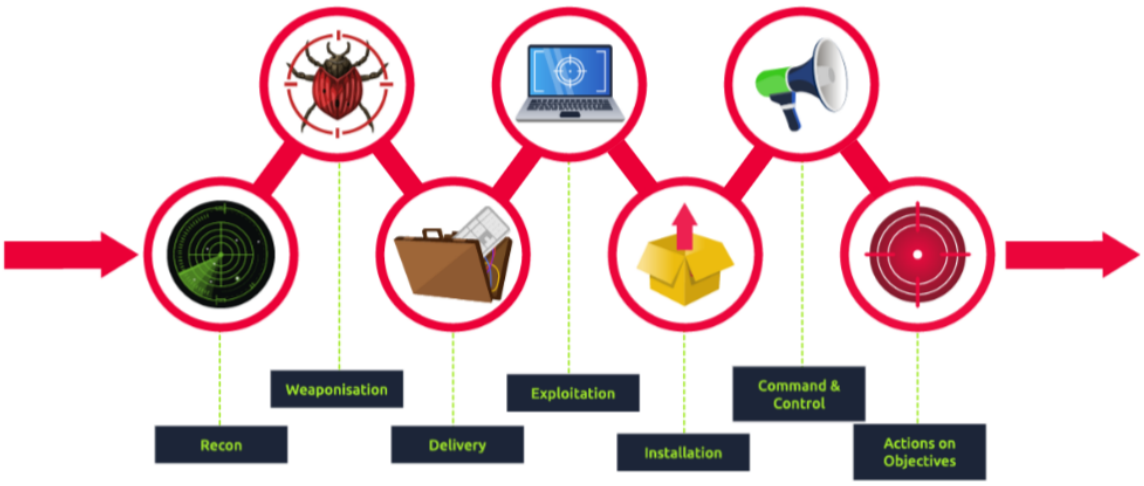
Cyber Kill Chain

-Đế Tọa-



I. Overview

Thuật ngữ "kill chain" là một khái niệm quân sự liên quan đến cấu trúc của một cuộc tấn công. Nó bao gồm việc xác định mục tiêu, quyết định và ra lệnh tấn công mục tiêu, và cuối cùng là phá hủy mục tiêu.

Nhờ Lockheed Martin, một công ty an ninh toàn cầu và hàng không vũ trụ, đã thiết lập khung Cyber Kill Chain® cho ngành công nghiệp an toàn mạng vào năm 2011 dựa trên khái niệm quân sự. Khung này xác định các bước được sử dụng bởi đối thủ hoặc các bên hành động xấu trong không gian mạng. Để thành công, một đối thủ cần phải trải qua tất cả các giai đoạn của Kill Chain. Chúng ta sẽ đi qua các giai đoạn tấn công và giúp bạn hiểu rõ hơn về đối thủ và các kỹ thuật mà họ sử dụng trong cuộc tấn công để tự bảo vệ.

Vậy tại sao việc hiểu cách Cyber Kill Chain hoạt động lại quan trọng?

Cyber Kill Chain sẽ giúp bạn hiểu và bảo vệ chống lại các cuộc tấn công ransomware, vi phạm an ninh cũng như Mối Đe Dọa Vững Vững và Tiên Tiến (APTs). Bạn có thể sử dụng Cyber Kill Chain để đánh giá an ninh mạng và hệ thống của bạn bằng cách xác định các điều khiển an ninh bị thiếu và đóng các khe bảo mật cụ thể dựa trên cơ sở hạ tầng của công ty bạn.

Bằng cách hiểu rõ về Kill Chain như một Chuyên viên SOC, Nghiên cứu An ninh, Người săn mối đe dọa hoặc Người phản ứng sự cố, bạn sẽ có khả năng nhận diện những cố gắng xâm nhập và hiểu rõ mục tiêu và mục đích của kẻ xâm nhập.

Chúng ta sẽ khám phá các giai đoạn tấn công sau đây trong phòng học này:

1. Thu thập thông tin (Reconnaissance)
2. Vũ khí hóa (Weaponization)
3. Phân phối (Delivery)
4. Tận dụng (Exploitation)
5. Cài đặt (Installation)
6. Kiểm soát và Điều khiển (Command & Control)
7. Thực hiện mục tiêu (Actions on Objectives)

Mục tiêu học: Trong phòng học này, bạn sẽ tìm hiểu về từng giai đoạn của Khung Cyber Kill Chain, ưu và nhược điểm của Cyber Kill Chain truyền thống.

Kết quả: Kết quả là bạn sẽ sẵn sàng nhận biết các giai đoạn hoặc các giai đoạn của cuộc tấn công thực hiện bởi một đối thủ và có khả năng phá vỡ "kill chain."

II. Theory

1. Reconnaissance

Để hiểu về thu thập thông tin là gì từ quan điểm của kẻ tấn công, đầu tiên, hãy xác định thuật ngữ thu thập thông tin.

Thu thập thông tin là việc khám phá và thu thập thông tin về hệ thống và nạn nhân. Giai đoạn thu thập thông tin là giai đoạn lên kế hoạch cho kẻ thù.

OSINT (Open-Source Intelligence - Tình báo nguồn mở) cũng nằm trong thu thập thông tin. **OSINT** là bước đầu tiên mà một kẻ tấn công cần hoàn thành để thực hiện các giai đoạn tiếp theo của một cuộc tấn công. Kẻ tấn công cần nghiên cứu nạn nhân bằng cách thu thập mọi thông tin có sẵn về công ty và nhân viên của nó, chẳng hạn như kích thước của công ty, địa chỉ email, số điện thoại từ các nguồn công khai để xác định mục tiêu tốt nhất cho cuộc tấn công.

Bạn cũng có thể tìm hiểu thêm về OSINT từ bài viết của Varonis, "What is OSINT?"

Hãy xem xét từ quan điểm của kẻ tấn công, người ban đầu không biết công ty nào mình muốn tấn công.

Dưới đây là kịch bản: Một kẻ tấn công tự đặt tên là "Megatron" quyết định thực hiện một cuộc tấn công rất phức tạp mà anh ấy đã lên kế hoạch từ nhiều năm nay; anh ấy đã nghiên cứu và nghiên cứu các công cụ và kỹ thuật khác nhau có thể giúp anh ấy đạt đến giai đoạn cuối của Cyber Kill Chain. Nhưng trước hết, anh ấy cần bắt đầu từ giai đoạn quân sự.

Để hoạt động trong giai đoạn này, kẻ tấn công sẽ cần thực hiện OSINT. Hãy xem xét việc thu thập Email.

Thu thập Email là quá trình lấy địa chỉ email từ các dịch vụ công cộng, trả phí hoặc miễn phí. Kẻ tấn công có thể sử dụng thu thập địa chỉ email cho một cuộc tấn công lừa đảo (loại cuộc tấn công kỹ thuật xã hội được sử dụng để đánh cắp dữ liệu nhạy cảm, bao gồm thông tin đăng nhập và số thẻ tín dụng). Kẻ tấn công sẽ có một kho vũ khí lớn của các công cụ có sẵn cho mục đích quân sự. Dưới đây là một số trong số chúng:

- theHarvester - ngoài việc thu thập email, công cụ này cũng có khả năng thu thập tên, subdomains, IPs và URLs sử dụng nhiều nguồn dữ liệu công cộng.
- Hunter.io - đây là một công cụ săn email giúp bạn có được thông tin liên quan đến tên miền.
- OSINT Framework - OSINT Framework cung cấp bộ công cụ OSINT dựa trên nhiều danh mục khác nhau.

Kẻ tấn công cũng sẽ sử dụng các trang web truyền thông xã hội như LinkedIn, Facebook, Twitter và Instagram để thu thập thông tin về một nạn nhân cụ thể anh ấy muốn tấn công hoặc công ty. Thông tin được tìm thấy trên truyền thông xã hội có thể hữu ích cho kẻ tấn công thực hiện cuộc tấn công lừa đảo.

Question and Answer

What is the name of the Intel Gathering Tool that is a web-based interface to the common tools and resources for open-source intelligence?

OSINT Framework

What is the definition for the email gathering process during the stage of reconnaissance?

Email harvesting

2. Weaponization

Sau giai đoạn Reconnaissance thành công, "Megatron" sẽ bắt đầu xây dựng một "vũ khí hủy diệt". Anh ấy sẽ thích không tương tác trực tiếp với nạn nhân và thay vào đó, anh ấy sẽ tạo ra một "weaponizer" mà theo Lockheed Martin, kết hợp malware và exploit thành một gói payload có thể chuyển giao. Hầu hết các kẻ tấn công thường sử dụng các công cụ tự động để tạo ra malware hoặc tham khảo DarkWeb để mua malware. Những đối tượng phức tạp hơn hoặc các nhóm APT (Advanced Persistent Threat) được tài trợ bởi quốc gia thì thường viết malware tùy chỉnh của mình để làm cho mẫu malware trở nên độc đáo và tránh phát hiện trên mục tiêu.

Hãy định nghĩa một số thuật ngữ trước khi phân tích giai đoạn Weaponization.

- **Malware (Phần mềm độc hại):** Là một chương trình hoặc phần mềm được thiết kế để gây hại, làm gián đoạn, hoặc có quyền truy cập trái phép vào máy tính.
- **Exploit (Khai thác):** Là một chương trình hoặc mã lập trình tận dụng lỗ hổng hoặc điểm yếu trong ứng dụng hoặc hệ thống.
- **Payload (Gói payload):** Là một mã độc hại mà kẻ tấn công chạy trên hệ thống.

Tiếp tục với đối thủ của chúng ta, "Megatron" chọn...

"Megatron" chọn mua một payload đã được viết sẵn từ một người khác trên DarkWeb, để anh ấy có thể dành nhiều thời gian hơn cho các giai đoạn khác.

Trong giai đoạn Weaponization, kẻ tấn công sẽ:

1. Tạo một tài liệu Microsoft Office bị nhiễm chứa một macro độc hại hoặc các kịch bản VBA (Visual Basic for Applications). Nếu bạn muốn tìm hiểu về macro và VBA, hãy tham khảo bài viết "Intro to Macros and VBA For Script Kiddies" của TrustedSec.
2. Kẻ tấn công có thể tạo ra một payload độc hại hoặc một loại worm rất phức tạp, cài đặt nó trên ổ đĩa USB, và sau đó phân phối chúng ở nơi công cộng.
3. Kẻ tấn công sẽ chọn các kỹ thuật Command and Control (C2) để thực hiện các lệnh trên máy của nạn nhân hoặc chuyển giao thêm payloads. Bạn có thể đọc thêm về các kỹ thuật C2 trên MITRE ATT&CK.
4. Kẻ tấn công sẽ chọn một backdoor implant (cách truy cập vào hệ thống máy tính, bao gồm việc né tránh các cơ chế bảo mật).

Question and Answer

This term is referred to as a group of commands that perform a specific task. You can think of them as subroutines or functions that contain the code that most users use to automate routine tasks. But malicious actors tend to use them for malicious purposes and include them in Microsoft Office documents. Can you provide the term for it?

macro

3.Delivery

Giai đoạn Delivery là khi "Megatron" quyết định chọn phương thức truyền tải payload hoặc malware. Anh ấy có nhiều lựa chọn để chọn:

1. **Phishing qua email:** Sau khi thực hiện quân sự và xác định mục tiêu cho cuộc tấn công, kẻ tấn công sẽ tạo ra một email độc hại dành cho một người cụ thể (cuộc tấn công spearphishing) hoặc nhiều người trong công ty. Email sẽ chứa một payload hoặc malware. Ví dụ, "Megatron" có thể biết được rằng Nancy từ bộ phận Kinh doanh ở công ty A thường xuyên thích các bài đăng trên LinkedIn từ Scott, một quản lý Dịch vụ ở công ty B. Anh ấy có thể đoán rằng họ liên lạc với nhau qua email công việc. "Megatron" sẽ tạo một email bằng tên và họ của Scott, làm cho miền trông giống như công ty mà Scott đang làm việc. Kẻ tấn công sau đó sẽ gửi một email giả mạo "Hóa đơn" cho Nancy, chứa payload.
2. **Phân phối USB bị nhiễm ở các địa điểm công cộng như quán cà phê, bãi đỗ xe, hoặc trên đường phố:** Kẻ tấn công có thể quyết định thực hiện một Cuộc tấn công USB Drop phức tạp bằng cách in logo của công ty lên USB và gửi chúng đến công ty khi giả vờ là một khách hàng gửi quà tặng USB. Bạn có thể đọc về một trong những cuộc tấn công tương tự này trên CSO Online "Nhóm tội phạm mạng gửi USB dongle độc hại đến các công ty đã nhắm mục tiêu."
3. **Tấn công Watering Hole (mục tiêu uống nước):** Một cuộc tấn công Watering Hole là một cuộc tấn công được thiết kế để nhắm vào một nhóm cụ thể người bằng cách xâm phạm trang web họ thường xuyên truy cập và sau đó chuyển hướng họ đến trang web độc hại theo sự lựa chọn của kẻ tấn công. Kẻ tấn công sẽ tìm kiếm lỗ hổng đã biết trên trang web và cố gắng khai thác nó. Kẻ tấn công sẽ khuyến khích nạn nhân truy cập trang web bằng cách gửi email "vô hại" chỉ đến URL độc hại để làm cho cuộc tấn công hoạt động hiệu quả hơn. Sau khi truy cập trang web, nạn nhân sẽ không cố ý tải xuống malware hoặc một ứng dụng độc hại lên máy tính của họ. Loại tấn công này được gọi là tải xuống từ xa. Một ví dụ có thể là một cửa sổ pop-up độc hại yêu cầu tải xuống một tiện ích mở rộng trình duyệt giả mạo.

Question and Answer

What is the name of the attack when it is performed against a specific group of people, and the attacker seeks to infect the website that the mentioned group of people is constantly visiting.

watering hole attack

4.Exploitation

Để có quyền truy cập vào hệ thống, một kẻ tấn công cần khai thác lỗ hổng. Trong giai đoạn này, "Megatron" trở nên sáng tạo một chút - anh ấy tạo ra hai email lừa đảo, một chứa một liên kết lừa đảo đến một trang đăng nhập Office 365 giả mạo và một cái khác chứa một tệp đính kèm macro sẽ thực thi ransomware khi nạn nhân mở nó. "Megatron" thành công chuyển giao những thủ đoạn của mình và đưa ra hai nạn nhân nhấp vào liên kết độc hại và mở tệp độc hại.

Sau khi có quyền truy cập vào hệ thống, kẻ tấn công có thể khai thác các lỗ hổng phần mềm, hệ thống hoặc dựa trên máy chủ để leo thang đặc quyền hoặc di chuyển ngang. Theo CrowdStrike, di chuyển ngang đề cập đến các kỹ thuật mà một kẻ tấn công sử dụng sau khi đạt được quyền truy cập ban đầu vào máy của nạn nhân để di chuyển sâu hơn vào mạng để thu thập dữ liệu nhạy cảm.

Nếu bạn muốn tìm hiểu thêm về các lỗ hổng dựa trên máy chủ hoặc dựa trên web, vui lòng tham khảo phòng **TryHackMe OWASP Top 10**.

Kẻ tấn công cũng có thể áp dụng "Zero-day Exploit" ở giai đoạn này. Theo FireEye, "zero-day exploit hoặc zero-day vulnerability là một thủ đoạn chưa biết đến trong thực tế mà tiết lộ một lỗ hổng trong phần mềm hoặc phần cứng và có thể tạo ra vấn đề phức tạp trước khi bất kỳ ai nhận ra điều gì đã sai. Một zero-day exploit không để lại bất kỳ cơ hội phát hiện nào từ đầu."

Dưới đây là các ví dụ về cách một kẻ tấn công thực hiện việc khai thác:

1. Nạn nhân kích hoạt thủ đoạn bằng cách mở tệp đính kèm email hoặc nhấp vào liên kết độc hại.
2. Sử dụng zero-day exploit.
3. Khai thác lỗ hổng phần mềm, phần cứng, hoặc thậm chí lỗ hổng con người.
4. Kẻ tấn công kích hoạt thủ đoạn cho các lỗ hổng dựa trên máy chủ.

Question and Answer

Can you provide the name for a cyberattack targeting a software vulnerability that is unknown to the antivirus or software vendors?

zero-day

5.Installation

Như bạn đã học từ giai đoạn Weaponization, backdoor cho phép kẻ tấn công bypass các biện pháp bảo mật và giấu quyền truy cập. Một backdoor cũng được biết đến là một điểm truy cập.

Khi kẻ tấn công có quyền truy cập vào hệ thống, anh ấy muốn có khả năng truy cập lại hệ thống nếu anh ấy mất kết nối hoặc nếu anh ấy bị phát hiện và quyền truy cập ban đầu bị gỡ bỏ, hoặc nếu hệ thống sau đó được vá lỗi. Anh ấy sẽ không còn quyền truy cập nếu hệ thống được vá. Đó là lúc kẻ tấn công cần cài đặt một backdoor kiên trì. Một backdoor kiên trì sẽ cho phép kẻ tấn công truy cập vào hệ thống mà anh ấy đã xâm nhập trong quá khứ. Bạn có thể tham khảo phòng Windows Persistence Room trên TryHackMe để biết cách một kẻ tấn công có thể đạt được sự kiên trì trên Windows.

Sự kiên trì có thể đạt được thông qua:

1. **Cài đặt web shell trên máy chủ web:** Web shell là một đoạn mã độc hại được viết bằng các ngôn ngữ lập trình phát triển web như ASP, PHP, hoặc JSP được kẻ tấn công sử dụng để duy trì quyền truy cập vào hệ thống đã bị tấn công. Do sự đơn giản của web shell và định dạng tệp tin (.php, .asp, .aspx, .jsp, vv.) có thể khó phát hiện và có thể được phân loại như lành tính.
2. **Cài đặt backdoor trên máy tính của nạn nhân:** Ví dụ, kẻ tấn công có thể sử dụng Meterpreter để cài đặt backdoor trên máy tính của nạn nhân. Meterpreter là một tải trọng của Metasploit Framework cung cấp một dòng lệnh tương tác từ đó kẻ tấn công có thể tương tác với máy tính của nạn nhân từ xa và thực thi mã độc hại.
3. **Tạo hoặc sửa đổi dịch vụ Windows:** Kỹ thuật này được biết đến là T1543.003 trên MITRE ATT&CK (MITRE ATT&CK® là một cơ sở dữ liệu kiến thức về các chiến thuật và kỹ thuật của đối thủ dựa trên các tình huống thực tế). Kẻ tấn công có thể tạo hoặc sửa đổi các dịch vụ Windows để thực thi các đoạn mã độc hại hoặc payloads định kỳ như một phần của sự kiên trì. Kẻ tấn công có thể sử dụng các công cụ như sc.exe (sc.exe cho phép bạn Tạo, Bắt đầu, Dừng, Truy vấn, hoặc Xóa bất kỳ Dịch vụ Windows nào) và Reg để sửa đổi cấu hình dịch vụ. Kẻ tấn công cũng có thể che đậy payload độc hại bằng cách sử dụng tên dịch vụ được biết đến liên quan đến Hệ điều hành hoặc phần mềm hợp lệ.
4. **Thêm mục vào "run keys" cho payload độc hại trong Registry hoặc thư mục Startup:** Bằng cách làm đó, payload sẽ thực thi mỗi khi người dùng đăng nhập vào máy tính. Theo MITRE ATT&CK, có một vị trí thư mục khởi động cho các tài khoản người dùng cá nhân và một thư mục khởi động toàn hệ thống sẽ được kiểm tra bất kỳ tài khoản người dùng nào đăng nhập.

Trong giai đoạn này, kẻ tấn công cũng có thể sử dụng kỹ thuật Timestomping để tránh phát hiện từ các nhà điều tra pháp y và cũng để làm cho phần mềm độc hại xuất hiện như một phần của một chương trình hợp lệ. Kỹ thuật Timestomping cho phép kẻ tấn công sửa đổi các dấu thời gian của tệp tin, bao gồm thời gian sửa đổi, truy cập, tạo và thay đổi.

Question and Answer

Can you provide the technique used to modify file time attributes to hide new or changes to existing files?

Timestomping

Can you provide the technique used to modify file time attributes to hide new or changes to existing files?

web shell

6.Command & Control

Sau khi có sự kiên trì và thực thi malware trên máy tính của nạn nhân, "Megatron" mở kênh C2 (Command and Control) thông qua malware để điều khiển và kiểm soát nạn nhân từ xa. Thuật ngữ này còn được biết đến là C&C hoặc C2 Beaconing, là một loại giao tiếp độc hại giữa một máy chủ C&C và malware trên máy chủ bị nhiễm. Máy chủ bị nhiễm sẽ liên tục giao tiếp với máy chủ C2; đây cũng là nguồn gốc của thuật ngữ "beaconing".

Máy chủ bị nhiễm sẽ liên lạc với một máy chủ ngoại vi được thiết lập bởi kẻ tấn công để thiết lập một kênh điều khiển và kiểm soát. Sau khi thiết lập kết nối, kẻ tấn công có quyền kiểm soát đầy đủ máy tính của nạn nhân. Cho đến gần đây, IRC (Internet Relay Chat) là kênh C2 truyền thống được kẻ tấn công sử dụng. Điều này không còn đúng nữa, vì các giải pháp bảo mật hiện đại có thể dễ dàng phát hiện lưu lượng IRC độc hại.

Các kênh C2 phổ biến nhất được đối thủ sử dụng ngày nay bao gồm:

1. **Các giao thức HTTP trên cổng 80 và HTTPS trên cổng 443 -** Loại beaconing này kết hợp lưu lượng độc hại với lưu lượng hợp lệ và có thể giúp kẻ tấn công tránh qua tường lửa.
2. **DNS (Domain Name Server) -** Máy tính bị nhiễm thực hiện các yêu cầu DNS liên tục đến máy chủ DNS thuộc sở hữu của kẻ tấn công; loại giao tiếp C2 này còn

được biết đến là DNS Tunneling.

Quan trọng lưu ý rằng một đối thủ hoặc một máy chủ bị nhiễm khác có thể là chủ sở hữu của cơ sở hạ tầng C2.

Question and Answer

What is the C2 communication where the victim makes regular DNS requests to a DNS server and domain which belong to an attacker.

DNS Tunneling

7.Actions on Objectives (Exfiltration)

Sau khi trải qua sáu giai đoạn của cuộc tấn công, "Megatron" cuối cùng có thể đạt được mục tiêu của mình, điều này có nghĩa là thực hiện các hành động trên các mục tiêu ban đầu. Với quyền truy cập trực tiếp vào bàn phím, kẻ tấn công có thể đạt được những điều sau đây:

1. **Thu thập thông tin đăng nhập từ người dùng:**
2. **Thực hiện đặc quyền (đạt được quyền truy cập được nâng cao như quyền quản trị viên miền từ một máy trạm thông qua việc khai thác cấu hình sai lầm):**
3. **Dò tìm nội bộ (ví dụ, kẻ tấn công tương tác với phần mềm nội bộ để tìm ra các lỗ hổng của nó):**

4. **Lateral movement (Di chuyển ngang) qua môi trường của công ty:**
5. **Thu thập và rò rỉ dữ liệu nhạy cảm:**
6. **Xóa bỏ bản sao lưu và bản sao shadow (Shadow Copy là một công nghệ của Microsoft có thể tạo ra bản sao lưu, bản chụp của tệp tin hoặc các ổ đĩa máy tính):**
7. **Ghi đè hoặc hỏng dữ liệu:**

Những hành động này có thể gây hậu quả nặng nề đối với tổ chức bị tấn công và nói chung, làm suy giảm tính toàn vẹn, sự riêng tư và an ninh của hệ thống thông tin.

Question and Answer

Can you provide a technology included in Microsoft Windows that can create backup copies or snapshots of files or volumes on the computer, even when they are in use?

shadow copy

8.Task

- Không khó lắm
- flag là : THM{7HR347_1N73L_12_4w35om3}