Cybersecurity

Corso tenuto dalla Professoressa Federica Paci

Università degli Studi di Verona

Alessio Gjergji

Indice

Capitolo 1

Cyber Kill Chain

1.1 Introduzione

La funzione principale della **cybersecurity** è proteggere i dispositivi che utilizziamo e i servizi a cui accediamo da accessi non autorizzati, danni o abusi. Essa mira anche a prevenire l'accesso non autorizzato a grandi quantità di dati salvati sia sui dispositivi e online.

1.1.1 Principi fondamentali della cybersecurity

Gli elementi fondamentali della cybersecurity sono:

- **Confidenzialità**: garantisce che i dati siano accessibili solo a chi è autorizzato.
- **Integrità**: assicura che i dati non siano alterati da persone non autorizzate.
- **Disponibilità**: rende i dati accessibili quando necessario.
- **Autenticazione**: verifica l'identità di un utente per accertarne la legittimità.
- **Autorizzazione**: assicura che l'utente abbia i permessi necessari per accedere ai dati.
- **Safety**: sistemi progettati e funzionanti in modo sicuro.
- **Accountability**: garantisce che le azioni degli utenti siano tracciabili.

1.1.2 Asset

Definizione di Asset

Un **asset** è qualsiasi elemento che ha valore per un'organizzazione. Tra gli asset rientrano persone, dispositivi, sistemi `IT`, network, software e ogni altro elemento a cui si può attribuire un valore.

1.1.3 Concetti chiave della cybersecurity

- **Vulnerabilità**: un bug, difetto o debolezza di un'applicazione, sistema o servizio che potrebbe compromettere le sue proprietà di sicurezza.
- **Cyber Threat**: una potenziale minaccia che potrebbe sfruttare una vulnerabilità per compromettere un asset.
- **Attacco**: la concretizzazione di una minaccia (*cyber threat*) che impatta negativamente su un asset.
- **Threat Actor**: un'entità (*es. individuo, gruppo o organizzazione*) che sfrutta una vulnerabilità per attaccare un asset.
- **Rischio**: il livello di impatto sulle operazioni, gli asset dell'organizzazione, sugli individui, su altre organizzazioni o sulla reputazione, derivante dalla combinazione di una minaccia e della probabilità che questa si verifichi.
- **Security Controls**: misure di gestione e controlli tecnici prescritti per proteggere la confidenzialità, integrità e disponibilità di un sistema, dei suoi componenti, processi e dati.

1.2 Cyber Kill Chain

Definizione di Cyber Kill Chain

La **Cyber Kill Chain** è un modello che descrive le fasi di un attacco informatico, dalla fase di ricognizione fino a quella di azione.

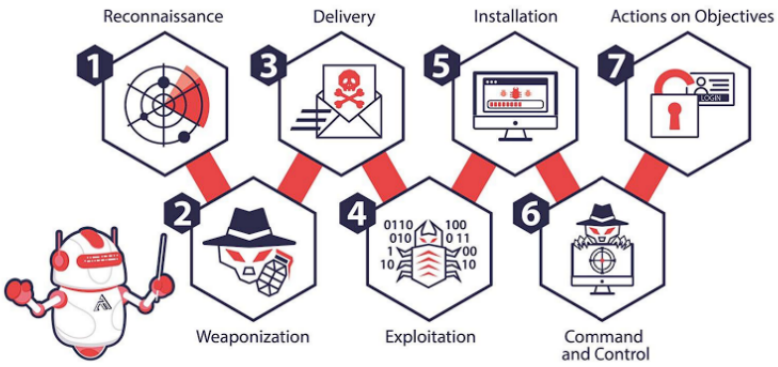

Figura 1.2.1: Cyber Kill Chain

1.2.1 Fasi della Cyber Kill Chain

1. **Reconnaissance**: fase in cui l'attaccante raccoglie informazioni sull'organizzazione, sui suoi asset e sulle vulnerabilità presenti. Questa fase può essere:

- **Passiva**: l'attaccante raccoglie informazioni da fonti pubbliche.
- **Attiva**: l'attaccante raccoglie informazioni tramite attività di scansione e sondaggio (`nmap`, *port scanning*).

2. **Weaponization**: fase in cui l'attaccante crea un payload malevolo e lo trasforma in un file eseguibile (*metasploit*, *air crack*).
3. **Delivery**: si seleziona in che modo trasportare l'exploit (*es. email, USB, social engineering*).
4. **Exploitation**: fase in cui il payload malevolo sfrutta una vulnerabilità per eseguire il codice malevolo (es. *buffer overflow*, *SQL injection*).
5. **Installation**: fase in cui si mantiene la persistenza nell'ambiente (*remote access trojan, powershell commands, DLL hijacking*). Si cerca anche di fare movimento laterale e spostarsi su altre macchine.
6. **Command and Control**: fase in cui si stabilisce un **canale di comando e controllo**, abbreviato in `C2`, in modo da manipolare la vittima, si apre quindi un canale di comunicazione a due vie tra l'attaccante e la vittima.
7. **Actions on Objectives**: fase in cui l'attaccante raggiunge i suoi obiettivi, come rubare dati o interrompere i servizi.

1.2.2 Trickbot

Trickbot

Un **Trickbot** è un trojan avanzato che si diffonde principalmente tramite email di phishing. Una volta scaricato inconsapevolmente dall'utente, Trickbot stabilisce un canale di comunicazione con un server di comando e controllo (`C2`), attraverso il quale l'attaccante può inviare comandi, distribuire Trickbot stesso o altri malware all'interno della rete compromessa.

1.3 `MITRE PREATT&CK` e `ATT&CK`

Definizione di MITRE ATT&CK

Il `MITRE ATT&CK` è un framework di tattiche e tecniche utilizzato per descrivere le fasi di un attacco informatico. Il framework è suddiviso in due parti: il `PREATT&CK` e l'`ATT&CK`.

È possibile mappare il `MITRE PREATT&CK` nelle fasi di reconnaissance e weaponization della *Cyber Kill Chain*, mentre l'`MITRE ATT&CK` corrisponde alle fasi di delivery, exploitation, installation, command and control, e actions on objectives.

1.3.1 MITRE PREATT&CK

Definizione di MITRE PREATT&CK

Il MITRE PREATT&CK raccoglie tutte le tattiche e le tecniche utilizzate nelle prime fasi di un attacco informatico. La struttura del framework è organizzata in colonne di tattiche, mentre le righe rappresentano le relative tecniche associate.

Ad esempio, la tattica *technical information gathering* rappresenta il processo mediante il quale un attaccante identifica informazioni critiche sul target, necessarie per pianificare efficacemente l'attacco.

Tra le tecniche di questa tattica troviamo **discover target logon/email address format**, che consiste nel determinare come sono strutturati i formati degli indirizzi email di una specifica organizzazione, ad esempio il dominio o il modello utilizzato.

1.3.2 MITRE ATT&CK

Definizione di MITRE ATT&CK

Il MITRE ATT&CK si concentra sulle tattiche e tecniche adottate durante le fasi operative di un attacco informatico.

MITRE ATT&CK matrix

La MITRE ATT&CK Matrix organizza le sue informazioni in colonne rappresentanti le tattiche e righe che descrivono le tecniche associate a tali tattiche. Le tattiche rappresentano ciò che un attaccante spera di ottenere, mentre le tecniche rappresentano come l'attaccante può raggiungere tali obiettivi.

Ad esempio, nell'ambito della tattica *Initial Access*, troviamo la tecnica di *phishing*, che consiste nel tentativo di ottenere informazioni sensibili o prendere il controllo di un sistema attraverso messaggi ingannevoli rivolti alla vittima. Se l'attacco è mirato, viene definito *spearphishing*, il quale a sua volta presenta delle sottotecniche. Una di queste è lo *spearphishing attachment*, in cui si invia un'email contenente un allegato malevolo progettato per ottenere informazioni sensibili o accesso al sistema. Gli allegati possono essere file eseguibili, PDF o documenti Office.

Per mitigare tali minacce, è possibile utilizzare strumenti come *network intrusion detection systems*, *email gateways* e antivirus, che generalmente sono in grado di rilevare allegati malevoli.

1.3.3 Tattiche e tecniche utilizzate da TrickBot

Analizziamo le tecniche dell'ATT&CK Matrix e come TrickBot le sfrutta nelle varie fasi della *cyber kill chain*:

- **Reconnaissance**: TrickBot utilizza tecniche come lo *spearphishing attachment* o lo *spearphishing link* per raccogliere informazioni e compromettere il bersaglio.

- **Execution**: Viene eseguito codice malevolo tramite tecniche come *scheduled task* o file *JavaScript* maligni.
- **Persistence**: Per mantenere l'accesso al sistema compromesso, TrickBot crea un servizio che si avvia automaticamente all'accensione della macchina.
- **Privilege Escalation**: L'attacco mira a ottenere privilegi maggiori sul sistema compromesso.
- **Defense Evasion**: TrickBot impiega diverse tecniche per eludere i sistemi di difesa, tra cui:
  - Offuscamento del codice;
  - Cifratura del malware;
  - Disattivazione di strumenti di sicurezza come Windows Defender.
- **Credential Access**: Include tecniche per la scoperta e il furto di credenziali.
- **Lateral Movement**: Movimento laterale all'interno della rete per compromettere ulteriori sistemi.
- **Collection**: Raccolta di dati sensibili dal sistema compromesso.
- **Command and Control**: Comunicazione tra il malware e il server di comando e controllo per ricevere istruzioni o inviare dati raccolti.
- **Exfiltration**: Estrazione dei dati sensibili verso server esterni controllati dall'attaccante.
- **Impact**: Tecniche per influenzare, sabotare o interrompere i sistemi compromessi.

1.3.4 Chi c'è dietro gli ultimi attacchi?

Dietro gli ultimi attacchi informatici troviamo tre principali tipologie di attori: cybercriminali, attori finanziati dallo Stato (*nation-state hackers*) e hacktivisti. Le origini principali di questi gruppi sono Russia e Cina, mentre i loro obiettivi principali includono gli Stati Uniti, seguiti dal Regno Unito. Le industrie più colpite sono i governi, i servizi finanziari e il settore tecnologico.

Cybercriminali

I cybercriminali sono mossi dall'interesse di ottenere profitti illegali. Tra gli attacchi tipici che eseguono troviamo:

- **Ransomware**: Blocco dei dati delle vittime in cambio di un riscatto.
- **Infostealers** (es. *Raccoon Stealer*): Software progettati per rubare informazioni sensibili.

- **Proxyjacking** (es. *Avrecon*): Una tipologia di attacco che sfrutta piattaforme di *proxyware*, le quali consentono agli utenti di guadagnare condividendo la propria connessione Internet con altri. Gli attaccanti monetizzano la larghezza di banda delle vittime sfruttando queste piattaforme.

Nation-State Hackers

Gli attori finanziati dallo Stato (*nation-state hackers*) sono interessati principalmente a:

- **Intelligence**: Raccolta di informazioni riservate.
- **Sabotaggio e Spionaggio**: Danni a infrastrutture critiche o spionaggio tecnologico e industriale.

Tra gli attacchi tipici eseguiti troviamo:

- Attacchi a infrastrutture critiche.
- Wipers: Malware progettati per distruggere i dati.
- Attacchi *DDoS*: Interruzione dei servizi tramite sovraccarico di traffico.

Hacktivisti

Gli hacktivisti sono motivati da visioni politiche, credi religiosi/sociali o ideologie terroristiche. Tra i principali attacchi da loro eseguiti troviamo:

- *DDoS*.
- Furti di dati (*data breaches*) o pubblicazioni di dati (*data leaks*).
- *Data wipers*.

Tra i gruppi più noti di hacktivisti ci sono *Anonymous*, *GhostSec* e *KillNet*.

1.3.5 Come operano gli attori?

Gli attori informatici utilizzano diverse tecniche e strumenti avanzati per raggiungere i loro obiettivi:

- **Attack-as-a-Service**: Gli attaccanti offrono servizi di attacco in cambio di un compenso (*fee*), permettendo a chiunque di "affittare" un attacco come servizio.
- **Compromissione dei dispositivi di rete**: L'accesso iniziale viene spesso ottenuto compromettendo dispositivi di rete. Strumenti come *Shodan*, *Censys* e *Kamerka* vengono utilizzati per individuare dispositivi esposti su Internet, come router o videocamere IP, spesso compromessi tramite credenziali di default o deboli.
- **Strumenti di offensive security**: Strumenti come *Metasploit* vengono utilizzati per condurre attacchi mirati.

- **Living Off The Land Binaries (LOLBins)**: Gli attaccanti utilizzano elementi di sistema legittimi, come processi nativi di Windows, per mascherare malware ed evitare il rilevamento.