ESERCITAZIONE W19D1(1)

EPICODE

Esercizio
Threat Intelligence & IOC

Traccia:
Creare un elenco di minacce comuni che possono colpire un'azienda, ad esempio phishing, malware, attacchi DDoS, furto di dati.

- Inizia raccogliendo informazioni sulle minacce alla sicurezza informatica, utilizzando fonti aperte, i siti web di sicurezza informatica e i forum di discussione.
- Analizza ciascuna minaccia in dettaglio, cercando di comprendere il modo in cui può essere utilizzata per compromettere la sicurezza informatica e i danni che può causare.
- Utilizza queste informazioni per creare un elenco delle minacce più comuni, tra cui malware, attacchi di phishing e attacchi DDoS aggiungendo tutte le informazioni raccolte dall'analisi.

1. Phishing:

Gli attaccanti inviano email o messaggi di testo che sembrano provenire da fonti legittime, come banche, istituzioni finanziarie o aziende con cui l'utente potrebbe avere un account. Questi messaggi spesso chiedono all'utente di fornire informazioni personali, come username, password, informazioni finanziarie o numeri di carta di credito. I link all'interno di tali messaggi possono indirizzare l'utente a siti web contraffatti progettati per rubare le loro credenziali o installare malware sui loro dispositivi.

2. Malware:

Il malware è un termine generico che si riferisce a software dannoso progettato per danneggiare o compromettere un sistema informatico. I tipi comuni di malware includono virus, worm, trojan, ransomware e spyware. Il malware può essere distribuito attraverso allegati di email, link dannosi, siti web compromessi o file scaricati da fonti non attendibili.

3. Attacchi DDoS (Distributed Denial of Service):

Gli attacchi DDoS mirano a sovraccaricare i server, i servizi online o le reti con un'elevata quantità di traffico dannoso. Questo traffico dannoso è spesso generato da una rete di dispositivi compromessi (botnet) controllati dagli aggressori. L'obiettivo è rendere i servizi inaccessibili agli utenti legittimi impedendo loro di accedere ai siti web o ai servizi online.

4. Furto di dati:

Gli hacker possono ottenere accesso non autorizzato ai sistemi dell'azienda per rubare informazioni sensibili come dati dei clienti, informazioni finanziarie, proprietà intellettuale o segreti commerciali. Il furto di dati può avvenire attraverso vulnerabilità nel sistema, accesso non autorizzato ai database o ai server, o tramite tecniche di social social engineering.

5. Attacchi di social engineering:

Gli attacchi di social engineering coinvolgono la manipolazione delle persone all'interno dell'azienda per ottenere informazioni riservate o accesso ai sistemi. Gli aggressori possono utilizzare tattiche come il phishing telefonico, l'invio di email fraudolente o l'interazione diretta con dipendenti per ottenere informazioni sensibili o compromettere la sicurezza dei sistemi.

6. Man-in-the-Middle (MitM) attacks:

Gli attacchi MitM si verificano quando un aggressore intercetta e manipola le comunicazioni tra due parti. Gli aggressori possono ottenere informazioni sensibili, come password o dati finanziari, o possono modificare le comunicazioni per scopi dannosi.

7.Attacchi Zero-Day:

Gli attacchi Zero-Day sfruttano vulnerabilità di sicurezza precedentemente sconosciute per le quali non esiste ancora una patch o un aggiornamento di sicurezza disponibile. Poiché non esiste una difesa nota contro tali attacchi, possono essere particolarmente pericolosi e dannosi per le aziende.

Queste minacce offrono solo una visione generale delle potenziali minacce alla sicurezza aziendale. Per proteggersi efficacemente, è necessario adottare un approccio multi-livello che comprenda misure tecniche, formazione degli utenti e l'implementazione di una solida politica di sicurezza informatica.