MALWARE & ATTACKS

Attacchi informatici e Malware più diffusi

Fonti:

- *Wikipedia*
- *Geopop*
- *Kaspersky*

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.

Curiosità
Servizio in down?

Figura 2: Fonte: PowerCert Animated Videos: DDoS Attack Explained

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**;

SPOOFING

DEFINIZIONE

Attacco informatico che può assumere varie forme e può essere perpetrato in un'infinità di modi. A prescindere dalle modalità adottate dai criminali informatici nell'usare questa tecnica, un qualsiasi attacco di spoofing è sempre caratterizzato da un elemento distintivo che lo rende particolarmente insidioso: viene sfruttata la fiducia delle potenziali vittime per accedere a dati, diffondere malware, sottrarre denaro, e perpetrare altri obiettivi malevoli dietro un **inganno** che, inizialmente, è tutt'altro che palese.

Curiosità
Scam Adviser

SPOOFING - ESEMPIO

Figura 3: Fonte Posteitaliane

SPOOFING - ESEMPIO

- **E-mail spoofing**: l'attaccante (**Spoofer**) maschera l'indirizzo del mittente di un'email utilizzando software specifico o creando mail che differiscono da quella originale per pochi caratteri simili.
- **Spoofing ID chiamante o SMS**: l'attaccante modifica il modo in cui appare il suo numero alle vittime contattate, così che a queste sembri che la chiamata provenga da un numero conosciuto (per esempio quello "ufficiale" della banca)
- **Web spoofing**: l'attaccante può creare un sito Web falso che sembra del tutto simile a quello utilizzato da una certa azienda.
- **IP spoofing**: l'attaccante modifica l'indirizzo IP di origine di un pacchetto o cela l'identità di un dispositivo facendo credere di avere un altro indirizzo IP.

Curiosità
Truffa del postino

SPOOFING - ESEMPIO

- **E-mail spoofing**: l'attaccante (**Spoofer**) maschera l'indirizzo del mittente di un'email utilizzando software specifico o creando mail che differiscono da quella originale per pochi caratteri simili.
- **Spoofing ID chiamante o SMS**: l'attaccante modifica il modo in cui appare il suo numero alle vittime contattate, così che a queste sembri che la chiamata provenga da un numero conosciuto (per esempio quello "ufficiale" della banca)
- **Web spoofing**: l'attaccante può creare un sito Web falso che sembra del tutto simile a quello utilizzato da una certa azienda.
- **IP spoofing**: l'attaccante modifica l'indirizzo IP di origine di un pacchetto o cela l'identità di un dispositivo facendo credere di avere un altro indirizzo IP.

Curiosità
Truffa del postino

SPOOFING - ESEMPIO

- **E-mail spoofing**: l'attaccante (**Spoofer**) maschera l'indirizzo del mittente di un'email utilizzando software specifico o creando mail che differiscono da quella originale per pochi caratteri simili.
- **Spoofing ID chiamante o SMS**: l'attaccante modifica il modo in cui appare il suo numero alle vittime contattate, così che a queste sembri che la chiamata provenga da un numero conosciuto (per esempio quello "ufficiale" della banca)
- **Web spoofing**: l'attaccante può creare un sito Web falso che sembra del tutto simile a quello utilizzato da una certa azienda.
- **IP spoofing**: l'attaccante modifica l'indirizzo IP di origine di un pacchetto o cela l'identità di un dispositivo facendo credere di avere un altro indirizzo IP.

Curiosità
Truffa del postino

SPOOFING - ESEMPIO

- **E-mail spoofing**: l'attaccante (**Spoofer**) maschera l'indirizzo del mittente di un'email utilizzando software specifico o creando mail che differiscono da quella originale per pochi caratteri simili.
- **Spoofing ID chiamante o SMS**: l'attaccante modifica il modo in cui appare il suo numero alle vittime contattate, così che a queste sembri che la chiamata provenga da un numero conosciuto (per esempio quello "ufficiale" della banca)
- **Web spoofing**: l'attaccante può creare un sito Web falso che sembra del tutto simile a quello utilizzato da una certa azienda.
- **IP spoofing**: l'attaccante modifica l'indirizzo IP di origine di un pacchetto o cela l'identità di un dispositivo facendo credere di avere un altro indirizzo IP.

Curiosità
Truffa del postino

PHISHING

DEFINIZIONE

Il phishing (variante di fishing, "**pescare**") è un tipo di attacco informatico effettuato principalmente tramite **email**, che ha l'obiettivo di farsi fornire dalla vittima dati personali o finanziari fingendo che l'email provenga da enti come banche, corrieri, piattaforme di streaming o di shopping online. Le email di phishing contengono **link** che, se cliccati, mettono la vittima a rischio di scaricare **malware** o consegnare nelle mani del truffatore dati sensibili, come utenze e password, dati bancari e personali.

Quiz
Sei in grado di riconoscere i tentativi di phishing?

PHISHING

Figura 4: Fonte Come riconoscere un'email di phishing e prevenire la truffa (Geopop)

Curiosità
Open-Source Phishing Framework

SOCIAL ENGINEERING

DEFINIZIONE

Il **social engineering** (ingegneria sociale) è una tecnica di manipolazione che **fa leva sull'errore umano** per ottenere informazioni private, credenziali di accesso o dati di valore. Nell'ambito del cybercrimine, queste truffe basate sullo "**human hacking**" tendono ad adescare gli ignari utenti inducendoli a esporre dati riservati, diffondere infezioni malware o concedere l'accesso a sistemi soggetti a restrizioni. Gli attacchi possono avvenire online, di persona o attraverso altre interazioni.

Curiosità
Check if your email address is in a data breach

SOCIAL ENGINEERING - FASI DELL'ATTACCO

1. **PREPARAZIONE**: l'attaccante raccoglie informazioni di carattere generale sulla vittima o su un gruppo più ampio a cui appartiene.
2. **INFILTRAZIONE**: l'attaccante stabilisce una relazione o da inizio a un'interazione, avviata conquistando la fiducia della vittima.
3. **SFRUTTAMENTO DELLA VITTIMA**: l'attaccante, dopo aver conquistato la fiducia della vittima e aver identificato un punto debole per sferrare l'attacco, sfrutta la vittima per effettuare il proprio attacco.
4. **INTERRUZIONE DEI CONTATTI**: l'attaccante infine interrompe i contatti dopo che la vittima ha compiuto l'azione desiderata.

SOCIAL ENGINEERING - FASI DELL'ATTACCO

1. **PREPARAZIONE**: l'attaccante raccoglie informazioni di carattere generale sulla vittima o su un gruppo più ampio a cui appartiene.
2. **INFILTRAZIONE**: l'attaccante stabilisce una relazione o da inizio a un'interazione, avviata conquistando la fiducia della vittima.
3. **SFRUTTAMENTO DELLA VITTIMA**: l'attaccante, dopo aver conquistato la fiducia della vittima e aver identificato un punto debole per sferrare l'attacco, sfrutta la vittima per effettuare il proprio attacco.
4. **INTERRUZIONE DEI CONTATTI**: l'attaccante infine interrompe i contatti dopo che la vittima ha compiuto l'azione desiderata.

SOCIAL ENGINEERING - FASI DELL'ATTACCO

1. **PREPARAZIONE**: l'attaccante raccoglie informazioni di carattere generale sulla vittima o su un gruppo più ampio a cui appartiene.
2. **INFILTRAZIONE**: l'attaccante stabilisce una relazione o da inizio a un'interazione, avviata conquistando la fiducia della vittima.
3. **SFRUTTAMENTO DELLA VITTIMA**: l'attaccante, dopo aver conquistato la fiducia della vittima e aver identificato un punto debole per sferrare l'attacco, sfrutta la vittima per effettuare il proprio attacco.
4. **INTERRUZIONE DEI CONTATTI**: l'attaccante infine interrompe i contatti dopo che la vittima ha compiuto l'azione desiderata.

SOCIAL ENGINEERING - FASI DELL'ATTACCO

1. **PREPARAZIONE**: l'attaccante raccoglie informazioni di carattere generale sulla vittima o su un gruppo più ampio a cui appartiene.
2. **INFILTRAZIONE**: l'attaccante stabilisce una relazione o da inizio a un'interazione, avviata conquistando la fiducia della vittima.
3. **SFRUTTAMENTO DELLA VITTIMA**: l'attaccante, dopo aver conquistato la fiducia della vittima e aver identificato un punto debole per sferrare l'attacco, sfrutta la vittima per effettuare il proprio attacco.
4. **INTERRUZIONE DEI CONTATTI**: l'attaccante infine interrompe i contatti dopo che la vittima ha compiuto l'azione desiderata.

SOCIAL ENGINEERING - CARATTERISTICHE

Gli attacchi di social engineering si basano sul ricorso alla persuasione e alla fiducia da parte dell'attaccante. Quando l'utente è vittima di queste tattiche, è maggiormente incline a effettuare azioni che altrimenti non compierebbe. Tra i tanti tipi di attacchi, la vittima potrebbe lasciarsi fuorviare dai seguenti comportamenti:

- **EMOZIONI ESASPERATE**: Paura, eccitazione, curiosità, rabbia, senso di colpa, tristezza.
- **URGENZA**: La vittima potrebbe essere indotta a compromettersi con il pretesto di un problema serio che richiede attenzione immediata.
- **FIDUCIA**: La credibilità è inestimabile ed essenziale in un attacco di social engineering. Dal momento che l'autore dell'attacco sta essenzialmente mentendo, la fiducia gioca un ruolo di primo piano.

Curiosità
L'hacker più famoso della storia

SOCIAL ENGINEERING - CARATTERISTICHE

Gli attacchi di social engineering si basano sul ricorso alla persuasione e alla fiducia da parte dell'attaccante. Quando l'utente è vittima di queste tattiche, è maggiormente incline a effettuare azioni che altrimenti non compierebbe. Tra i tanti tipi di attacchi, la vittima potrebbe lasciarsi fuorviare dai seguenti comportamenti:

- **EMOZIONI ESASPERATE**: Paura, eccitazione, curiosità, rabbia, senso di colpa, tristezza.
- **URGENZA**: La vittima potrebbe essere indotta a compromettersi con il pretesto di un problema serio che richiede attenzione immediata.
- **FIDUCIA**: La credibilità è inestimabile ed essenziale in un attacco di social engineering. Dal momento che l'autore dell'attacco sta essenzialmente mentendo, la fiducia gioca un ruolo di primo piano.

Curiosità
L'hacker più famoso della storia

SOCIAL ENGINEERING - CARATTERISTICHE

Gli attacchi di social engineering si basano sul ricorso alla persuasione e alla fiducia da parte dell'attaccante. Quando l'utente è vittima di queste tattiche, è maggiormente incline a effettuare azioni che altrimenti non compierebbe. Tra i tanti tipi di attacchi, la vittima potrebbe lasciarsi fuorviare dai seguenti comportamenti:

- **EMOZIONI ESASPERATE**: Paura, eccitazione, curiosità, rabbia, senso di colpa, tristezza.
- **URGENZA**: La vittima potrebbe essere indotta a compromettersi con il pretesto di un problema serio che richiede attenzione immediata.
- **FIDUCIA**: La credibilità è inestimabile ed essenziale in un attacco di social engineering. Dal momento che l'autore dell'attacco sta essenzialmente mentendo, la fiducia gioca un ruolo di primo piano.

Curiosità
L'hacker più famoso della storia

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**.

"L'unico vero sistema sicuro è un sistema spento, chiuso in una gettata di cemento, sigillato in una stanza rivestita di piombo protetta da guardie armate. Ma anche in questo caso ho i miei dubbi."