Università degli Studi di Salerno

Dipartimento di Informatica

Penetration Testing & Ethical Hacking

Fondamenti di Ethical Hacking

Parte 1

Arcangelo Castiglione
arcastiglione@unisa.it

Outline

- Sicurezza e Caratterizzazione degli Attacchi
- Storia dell'Hacking
- Caratterizzazione degli Hacker
- Ethical Hacking Plan
- I Dieci Comandamenti dell'Ethical Hacking

Outline

- **Sicurezza e Caratterizzazione degli Attacchi**
- Storia dell'Hacking
- Caratterizzazione degli Hacker
- Ethical Hacking Plan
- I Dieci Comandamenti dell'Ethical Hacking

Cosa si Intende per Sicurezza?

- **Sicurezza Completa:** combinazione sinergica di sicurezza **Fisica**, **Digitale** ed **Umana**

Cosa si Intende per Sicurezza?

Sicurezza Fisica

- Analisi di sicurezza perimetrale
- Identificazione di accessi alternativi
- Controlli basati su RFID/NFC
- Controlli tramite dispositivi biometrici
- Illuminazione
- Analisi delle abitudini delle guardie
- Controllo remoto tramite CCTV
- …

Sicurezza Digitale

- Analisi di sistemi perimetrali
- Analisi di server pubblici
- Controllo di domini interni
- Controllo di sistemi industriali
- …

Sicurezza Umana

- Controlli su Phishing di massa
- Controlli su Phishing mirati
- Controlli su Vishing
- Controlli su Malware
- Controlli su USB Bait
- Controlli su Impersonificazione
- …

Per garantire la sicurezza nelle diverse dimensioni (Fisica, Digitale ed Umana) vengono svolte diverse azioni

Cosa si Intende per Sicurezza?

- I tre tipi di sicurezza sono strettamente correlati
  - Dispositivi digitali sono spesso utilizzati per garantire l'accesso in determinate aree fisiche
  - Senza proteggere adeguatamente una determinata area fisica, tutti i dispositivi digitali potrebbero essere compromessi localmente

Violazione Sicurezza Fisica

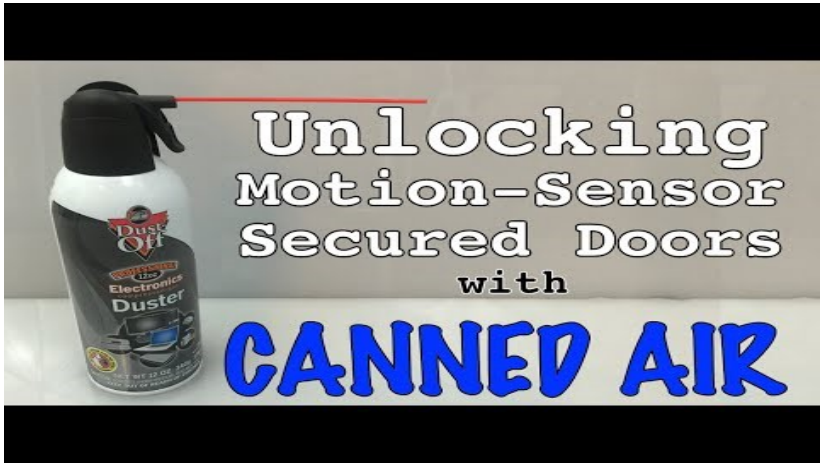
Esempi

- Analisi delle protezioni perimetrali per raccogliere informazioni sulle misure di sicurezza fisica messe in atto
  - Dopo l'intrusione si potrebbe collegare un dispositivo alla rete, estendendo la violazione della sicurezza fisica alla dimensione digitale

Violazione Sicurezza Fisica

Esempi

- Alcune porte possono essere aperte dall'interno grazie ad un sensore di movimento
  - Le porte non sono sovrapposte e possono essere aperte anche dall'esterno usando uno spray



https://www.youtube.com/watch?v=xcA7iXSNmZE

Violazione Sicurezza Fisica

Esempi

- Sfruttamento delle schede RFID/NFC
  - Diffuse in molti ambiti pubblici e privati
  - Utilizzano spesso configurazioni predefinite che consentono una facile duplicazione o clonazione

NFC

Violazione Sicurezza Fisica

Esempi

- Violazione di sistemi biometrici, guasti all'illuminazione, recinzioni facili da saltare, telecamere a circuito chiuso mal posizionate, etc

Violazione Sicurezza Digitale

- Tipicamente segue uno specifico pattern di attacco
  1. Utilizzo di tecniche per l'anonimia in rete (protocolli di tunneling, VPN, proxy, proxy chain, reti anonime, etc)
  2. Scelta del sistema (o dei sistemi) da attaccare
  3. Raccolta di informazioni sul sistema da attaccare
  4. Analisi delle vulnerabilità del sistema
  5. Realizzazione (o utilizzo) di strumenti per lo sfruttamento delle vulnerabilità rilevate (*exploit*)
     - Utilizzo di questi strumenti per accedere al sistema
  6. Realizzazione (o utilizzo) di strumenti per mantenere il controllo del sistema (*backdoor*) ed elevazione dei privilegi all'interno di esso

Durante il corso ci occuperemo prevalentemente di questi aspetti

Violazione Sicurezza Umana

Esempi

- Sviluppo di campagne di phishing
- Sviluppo di malware ad hoc
- Diffusione di pendrive USB infette (**USB bait**)
  - Una volta collegate ad un sistema da parte di utenti che hanno lecito accesso al sistema stesso, eseguiranno software dannoso

Tipi di Attacchi

- I sistemi sono sempre più complessi e vulnerabili
  - Il numero sempre crescente di dispositivi e tecnologie utilizzate aumenta la superficie di attacco
  - Più complesso è un sistema e più difficile risulta controllarlo

- In generale gli attacchi appartengono a tre categorie principali
  - **Attacchi Fisici**
  - **Attacchi Sintattici**
  - **Attacchi Semantici**

Attacchi Fisici

- Utilizzo di metodi tradizionali per «distruggere» i dati
  - Fiamme, Esplosivi, etc

- Possono anche riguardare l'intrusione in edifici ed il furto di apparecchiature
  - Anche rovistando tra la spazzatura è possibile trovare informazioni preziose (ad es., password, diagrammi di rete, note, etc)

Attacchi Sintattici

- Utilizzo di malware o di altre tipologie di software malevolo per violare o «disturbare» il normale funzionamento di un sistema

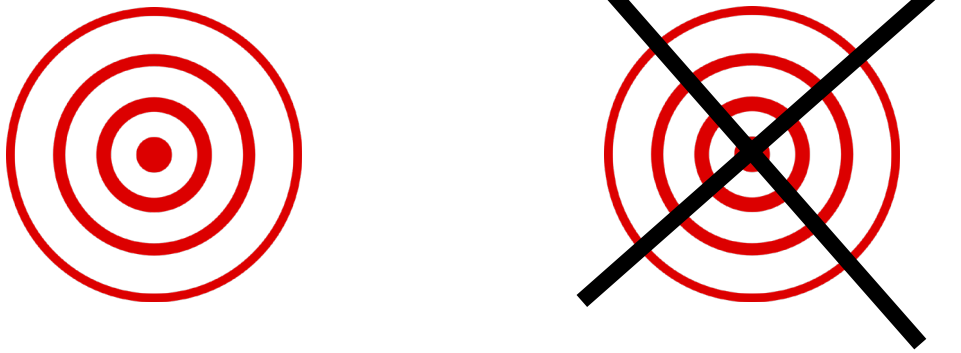
- Uno dei modi più comuni con cui viene eseguita questa forma di attacco è tramite e-mail
  - Ad es., attraverso campagne di phishing

Attacchi Semantici

- Fortemente relati al **social engineering**
- Utilizzo di tecniche per avvicinarsi al bersaglio (umano), acquisendone la fiducia e causando errori, malfunzionamenti o accessi non autorizzati al sistema
- L'attaccante è in grado di modificare le informazioni e distribuirle come genuine o diffondere informazioni inaccurate

Obiettivo degli Attacchi

- Tutti gli attacchi sono di solito classificati come
  - Mirati
  - Non Mirati (o Generici)



Attacchi Mirati

Pattern di Attacco

- L'attaccante
  1. Raccoglie tutte le informazioni disponibili sull'asset
  2. Analizza tali informazioni, per trovare un modo di accesso (**vettore**) all'asset
  3. Garantisce la persistenza dell'accesso, installando *backdoor* non rilevabili
  4. Ottiene il controllo di altri sistemi nell'asset, fino a raggiungere l'obiettivo finale (Tipicamente l'Accesso ai Dati 5.)
  6. Esce dall'asset

Attacchi Mirati

Svantaggi

- Richiedono tempo, motivazioni, denaro, competenze, esperienza, etc
  - Non tutti sono in grado di condurre/supportare tali attività

Attacchi Non Mirati (o Generici)

- Utilizzano malware o mezzi automatizzati, come campagne di phishing o di «massive exploitation»
  - **Esempio:** data una vulnerabilità per una specifica versione di WordPress, si potrebbe eseguire un exploit per violare tutti i server che hanno installato tale versione di WordPress

- Attacchi più economici e meno complessi, che possono causare danni molto gravi
  - Ad es., Ransomware

Attacchi
Come Rilevarli

- Alcuni «indizi» permettono di rilevare un attacco
  - Livello insolitamente alto del traffico di rete in uscita quando non si stanno effettuando download/upload
  - Livelli elevati di attività del disco
  - Comparsa di file o directory «sospette»
  - Servizi o processi sospetti
  - Grande quantità di dati in ingresso «bloccata» dal firewall
  - Trojan e backdoor rilevati dall'Antivirus (AV)
  - Etc

Attacchi

Come Proteggersi

- Non esiste una «regola generale», ma alcune linee guida possono essere di grande aiuto
  - Aggiornare costantemente i sistemi che si utilizzano
    - Sistema operativo, applicativi, etc
  - Utilizzare ed aggiornare costantemente gli strumenti di sicurezza
    - Antivirus, Firewall, IDS/IPS, etc
  - Disabilitare tutti i servizi di rete non necessari
  - Gestire l'accounting degli utenti secondo il *Principio del Privilegio Minimo*