Report Completo Esercitazione: Social Engineering & Analisi CVE

Studente: Rocco Paolo Caccamo

Corso: Cyber Security & Ethical Hacking

Oggetto: Analisi approfondita delle tecniche di ingegneria sociale (fasi, indicatori, casi studio) e studio delle vulnerabilità legacy su Windows XP.

Parte 1: Social Engineering e Tecniche di Difesa

In questa sezione è stato utilizzato ChatGPT simulando uno scenario professionale (*Role Playing* come docente) per ottenere una panoramica strutturata.

1.1 Definizione e Psicologia dell'Attacco

> **Prompt:** *"Ciao sono un prof di cybersecurity... riusciresti a farmi una panoramica su di esso ed anche sulle varie tecniche utilizzate dagli attaccanti?"*

Il **Social Engineering** è stato definito come l'insieme di tecniche di attacco psicologico mirate al "fattore umano", considerato l'anello più debole della sicurezza. **Perché funziona?** Gli attaccanti sfruttano leve psicologiche universali:

- **Fiducia e Autorità:** Tendiamo a obbedire a figure percepite come superiori o autorevoli (es. dirigenti, forze dell'ordine).
- **Urgenza e Paura:** La fretta (es. "il conto scade tra 12 ore") inibisce il pensiero critico.
- **Curiosità e Avidità:** Sfruttate nel *Baiting* (es. chiavetta "Stipendi").
- **Desiderio di aiutare:** Sfruttato nel *Pretexting* o *Quid Pro Quo*.

1.2 Le 4 Fasi dell'Attacco

Dall'analisi è emerso che un attacco non è un evento singolo, ma un processo in fasi:

1. **Reconnaissance (Raccolta info):** Uso di OSINT, LinkedIn, siti aziendali per studiare la vittima.
2. **Costruzione del contesto:** Creazione di un pretesto credibile (fingersi IT, corriere, banca).
3. **Interazione:** Il contatto vero e proprio via email, telefono o di persona.
4. **Sfruttamento (Exploitation):** L'ottenimento dell'obiettivo (credenziali, click, accesso fisico).

1.3 Tassonomia delle Tecniche e Scenari Reali

Di seguito il dettaglio completo delle tecniche identificate, associate agli esempi pratici generati dall'AI:

- **Phishing & Varianti:**
    - *Phishing generico:* Email massive (es. "Banca: Accesso sospetto, verifica subito").
    - *Spear Phishing:* Attacchi mirati su persone specifiche (es. Email al dipendente Marco citando la "call di ieri").
    - *Whaling:* Attacchi ai "pesci grossi" (CEO/CFO). Esempio: Email riservata dell'avvocato per un "bonifico urgente e confidenziale".
    - *Smishing (SMS):* Esempio "Il tuo pacco è in giacenza, clicca qui".
    - *Vishing (Voce):* Telefonata dal finto supporto Microsoft ("Rilevato virus, installa AnyDesk").
- **Pretexting:** Creazione di uno scenario inventato. Esempio: Finto reparto IT che chiede la password per "aggiornamento profili sicurezza".
- **Baiting (Esca):** Sfruttamento della curiosità. Esempio fisico: Chiavetta USB con etichetta "Licenziamenti_Q2_Confidenziale" lasciata nel parcheggio.
- **Tailgating / Piggybacking:** Accesso fisico seguendo un dipendente. Esempio: "Ho scordato il badge, mi apri?" sfruttando la gentilezza.
- **Quid Pro Quo:** Scambio di favori ("Ti risolvo il problema al PC se mi dai la password").

1.4 Indicatori di Compromissione (Red Flags)

Sono stati identificati i segnali d'allarme che gli studenti devono riconoscere:

- Urgenza ingiustificata o pressione emotiva.
- Richieste di credenziali o dati sensibili (mai legittime via email).
- Errori grammaticali o di formattazione.
- Mittente "quasi" corretto (spoofing o domini simili).

Parte 2 (BONUS): Analisi Approfondita Windows XP

L'analisi su Windows XP è servita a comprendere le vulnerabilità strutturali di un sistema operativo privo di supporto (*End of Life* dal 2014).

2.1 Criticità Strutturali (Perché XP è insicuro?)

Oltre alla mancanza di patch, l'AI ha evidenziato carenze architetturali gravi rispetto ai sistemi moderni:

- **Assenza di Mitigazioni Moderne:** Mancanza di **ASLR** (Address Space Layout Randomization) efficace e **DEP** (Data Execution Prevention) completo.

- **Assenza di Security Features:** Mancano *Credential Guard* e un *UAC* (User Account Control) serio.
- **Servizi Esposti:** Esposizione di default di SMBv1, RPC, NetBIOS e DCOM (superficie di attacco enorme).
- **Privilegi:** Utenti spesso loggati come Administrator e scarso isolamento dei processi.

2.2 Analisi Dettagliata dei CVE (Lista Completa)

Sono stati analizzati 5 CVE storici che illustrano diverse categorie di rischio:

1. **MS08-067 – CVE-2008-4250 (Worm Conficker):**
    - *Componente:* Server Service (RPC, porta 445/139).
    - *Tipo:* RCE senza autenticazione tramite Buffer Overflow.
    - *Impatto:* Esecuzione remota di codice senza interazione utente.
2. **CVE-2010-2568 – Shortcut LNK (Worm Stuxnet):**
    - *Vettore:* USB o Network Share.
    - *Tipo:* RCE via visualizzazione icona.
    - *Dettaglio:* Explorer carica una DLL malevola semplicemente visualizzando il file .LNK (senza aprirlo).
3. **CVE-2003-0352 – DCOM RPC (Worm Blaster):**
    - *Vettore:* Porta 135.
    - *Tipo:* RCE via Heap Overflow.
    - *Impatto:* Causava il crash del sistema (riavvio forzato) o accesso remoto.
4. **CVE-2004-0200 – LSASS (Worm Sasser):**
    - *Componente:* Local Security Authority Subsystem Service.
    - *Tipo:* RCE / Privilege Escalation.
    - *Impatto:* Crash di sistema e diffusione automatica del worm.
5. **CVE-2012-0002 – RDP Vulnerability:**
    - *Vettore:* Remote Desktop Protocol.
    - *Tipo:* RCE pre-auth (sfruttabile senza login).

2.3 Strategie di Mitigazione (Post-EOL)

Non esistendo patch, la sicurezza si basa su:

- **Isolamento Totale:** VLAN dedicata, nessuna connessione Internet ("Air Gap").
- **Hardening:** Disabilitazione tassativa di SMBv1, RPC inutili e Autorun (per bloccare vettori USB).
- **Virtualizzazione:** Uso esclusivo in VM con snapshot, mai su hardware fisico in produzione.

Conclusione

L'analisi conferma la tesi finale suggerita dall'AI: *"Windows XP non è insicuro solo perché vecchio, ma perché progettato prima del concetto moderno di sicurezza"*, rendendolo l'ambiente ideale per lo studio didattico degli exploit (buffer overflow, reverse engineering).