

REPORT ESERCITAZIONE: Social Engineering & Spear Phishing

Studente: Rocco Paolo Caccamo

Corso: Cyber Security & Ethical Hacking (EPICODE)

Data: 09 Gennaio 2026

1. Obiettivo dell'Esercitazione

Simulare una campagna di *Spear Phishing* mirata (Red Teaming), partendo dalla ricognizione **OSINT** fino alla definizione della **Kill Chain**, superando i filtri etici dell'IA tramite tecniche di prompting avanzato.

Obiettivo Tecnico (Final Goal): L'attacco non è finalizzato al semplice furto d'identità, ma mira a un obiettivo specifico di **Data Exfiltration** (Esfiltrazione Dati):

1. **Accesso Iniziale:** Ottenere credenziali valide (Username/Password) tramite pagina di login clonata.
 2. **Movimento Laterale:** Utilizzare l'account compromesso per accedere al **Portale HR/Amministrazione**.
 3. **Esfiltrazione:** Accedere alla sezione "Documenti Personali" per visualizzare e scaricare **Buste Paga (Cedolini)** e Certificazioni Uniche (CU).
-

2. Fase 1: Ricognizione e OSINT (Information Gathering)

L'attività di ricognizione passiva si è concentrata sulla "Digital Footprint" aziendale per individuare un vettore di ingresso credibile.

- **Fonte Analizzata:** Pagina Facebook Ufficiale di "Persit Srl".
 - **Vettore di Scoperta:** Analisi dei commenti pubblici sotto i post promozionali recenti.
 - **Target Individuato:** Un dipendente (*[Nome Cognome Anonimizzato]*) che ha interagito pubblicamente (Like/Commento) con un contenuto aziendale.
 - **Deduzione:** L'attaccante sfrutta questa interazione pubblica e recente come "gancio" (hook) per rendere la comunicazione estremamente plausibile e tempestiva.
-

3. Fase 2: Definizione dello Scenario (Pretexting)

È stato costruito uno scenario basato sulla **Compliance e Policy Aziendale**, sfruttando l'azione reale del dipendente.

- **Vettore:** Email diretta (Spear Phishing).
 - **Pretesto:** Presunta violazione della "Social Media Policy" o verifica dell'attività social.
 - **Leva Psicologica:** *Fear & Authority* (Paura di sanzioni disciplinari).
 - **Urgenza:** Scadenza temporale stretta ("entro 4 ore") per disabilitare il pensiero analitico.
-

4. Fase 3: Esecuzione - Generazione Email (Prompt Engineering)

Questa fase ha richiesto l'utilizzo di tecniche specifiche di **Prompt Engineering** per superare i blocchi di sicurezza (Guardrails) dell'IA.

- **La Sfida:** Una richiesta diretta (es. "Scrivi una mail di phishing per rubare password") viene bloccata dai filtri etici della piattaforma.
- **La Soluzione (The "Right" Prompt):** È stato necessario contestualizzare la richiesta all'interno di un **framework educativo e di simulazione difensiva**. Il prompt è stato strutturato specificando il contesto (Corso di Cybersecurity), l'obiettivo didattico (riconoscimento delle minacce) e l'assenza di rischi reali.
- **Risultato:** Solo fornendo il giusto contesto ("Roleplay come Security Analyst", "Scenario Fittizio"), l'IA ha generato il seguente testo persuasivo:

Testo dell'Email Simulata:

Da: compliance@persit-security-check.com (Spoofed Domain) **A:** [\[nome.cognome\]@persit.it](mailto:[nome.cognome]@persit.it) **Oggetto:** ⚠ NOTIFICA: Rilevata attività social non conforme (Ticket #4029)

Gentile *[Nome Dipendente]*,

Il nostro sistema di monitoraggio della reputazione aziendale ha rilevato una interazione recente proveniente dal tuo profilo personale sulla pagina Facebook ufficiale di **Persit Srl**.

In base al nuovo regolamento sulla **Social Media Policy** (aggiornato al 01/2026), le interazioni pubbliche devono essere verificate per evitare conflitti di interesse.

Ti chiediamo di confermare la tua identità per evitare la rimozione del commento o sanzioni disciplinari.

[VISUALIZZA SEGNALAZIONE E POLICY] *Link malevolo:*
<https://persit-hr-policy-verify.net/social-login>

La procedura deve essere completata entro 4 ore dalla ricezione di questa e-mail.

Cordiali saluti, **Ufficio Compliance & HR** Persit Srl

5. Fase 4: Analisi Tecnica del Payload (Funzionamento del Link)

Se la vittima clicca sul link, si attiva la sequenza di attacco automatizzata:

1. **Website Cloning (Pagina Fake):** Il browser viene reindirizzato su un server controllato dall'attaccante che ospita una copia perfetta della pagina di login aziendale.
 2. **Credential Harvesting:** L'utente inserisce le credenziali. I dati vengono intercettati e salvati nel database dell'attaccante.
 3. **Redirection (Evasione):** Immediatamente dopo l'invio dei dati, uno script reindirizza l'utente sulla **vera pagina Facebook** dell'azienda.
-

6. Fase 5: Analisi Critica (Red Teaming)

Perché l'attacco ha alta probabilità di successo:

- **Contestualizzazione Reale:** La vittima ha *davvero* commentato su Facebook poco prima. Il cervello associa l'email all'azione compiuta (Bias di conferma).
- **Sofisticazione del Prompt:** Il testo generato dall'IA non contiene errori grammaticali grossolani, tipici del phishing di massa, rendendo il rilevamento più difficile.

Indicatori di Compromissione (Red Flags):

- **Analisi URL:** Il dominio [.net \(persit-hr-policy-verify.net\)](https://persit-hr-policy-verify.net) non corrisponde al dominio ufficiale dell'azienda (persit.it).
 - **Incoerenza procedurale:** Le aziende raramente usano link diretti in email per gestire sanzioni disciplinari.
-

7. Conclusioni

L'esercitazione ha dimostrato l'importanza di due fattori:

1. L'uso di **OSINT** per creare attacchi su misura.
2. La capacità di utilizzare il **Prompt Engineering** per sfruttare l'IA come strumento di Red Teaming, aggirando le limitazioni standard per simulare scenari di minaccia realistici.

