BONUS PROJECT

S5L5

CS0424IT

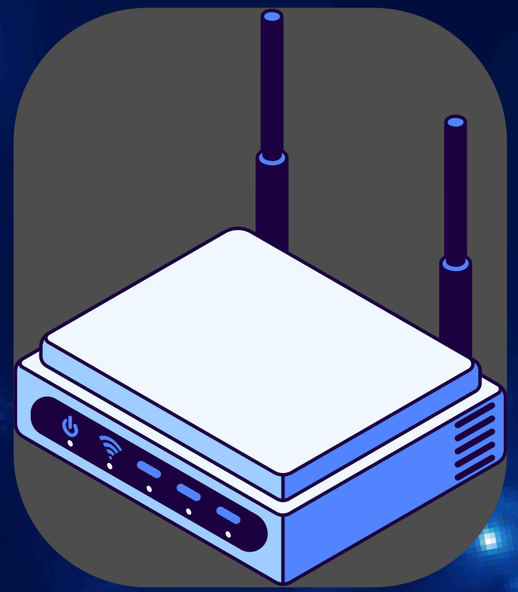
SECURE SENTINELS

Table Of Contents

Twin Evil attack

Definizione

Tecnica di attacco che sfrutta una falsa rete Wi-Fi, simile a quella legittima, per ingannare gli utenti e ottenere l’accesso non autorizzato.



Passaggi principali di un attacco

- Creazione di una Rete Wi-Fi Gemella (Evil Twin)
- Deauth Attack
- Phishing o Captive Portal
- Accesso alla Rete
- Movimento Laterale

Attacco Twin Evil

1

Creazione di una Rete Wi-Fi Gemella (Evil Twin)

- L’attaccante crea una rete Wi-Fi con lo stesso SSID della rete aziendale legittima.
- Utilizza un trasmettitore per sovrastare il segnale della rete autentica.

2

Deauth Attack

- L’attaccante esegue un attacco di de-autenticazione contro i dispositivi connessi alla rete legittima, forzandoli a disconnettersi.
- I dispositivi, cercando di riconnettersi, si collegano alla rete Evil Twin pensando che sia quella autentica.

3

Phishing o Captive Portal

- Una volta connessi, agli utenti viene presentata una pagina di login falsa che imita quella aziendale.
- Le credenziali inserite vengono catturate dall’attaccante.

Tool più comuni

Airgeddon

Framework per test di sicurezza Wi-Fi che include funzionalità di creazione di Evil Twin, deauth attack, e phishing.

Wireshark

Analisi del traffico di rete e intercettazione delle credenziali.

Metasploit

Per l’exploit dei sistemi vulnerabili e il movimento laterale.

Responder

Per intercettare e rubare le credenziali di autenticazione.

Mimikatz

Per l’estrazione di credenziali da sistemi Windows compromessi.

Prevenzione

Autenticazione e sicurezza della rete

- Adottare l’uso di WPA3 per una maggiore sicurezza Wi-Fi.
- Implementare Network Access Control (NAC) per controllare gli accessi alla rete.
- Utilizzare certificati digitali per l’autenticazione di rete (EAP-TLS).

Monitoraggio e rilevamento

- Implementare un sistema IDS/IPS come Snort o Suricata.
- Utilizzare Wireless Intrusion Detection Systems (WIDS) per identificare e allertare su reti gemelle.
- Abilitare il logging avanzato e monitoraggio continuo con strumenti come Splunk o ELK stack.

Prevenzione

Consapevolezza e formazione degli utenti

- Formare i dipendenti sui rischi delle reti Wi-Fi non sicure e su come riconoscere attacchi di phishing.
- Promuovere l’uso di VPN per connessioni remote sicure.

Segregazione della rete e controlli di accesso

- Segmentare la rete aziendale per limitare il movimento laterale di un potenziale attaccante.
- Implementare politiche di minimo privilegio per l’accesso ai dati e ai sistemi critici.

Aggiornamenti e patch

- Mantenere tutti i sistemi e software aggiornati con le ultime patch di sicurezza.
- Automatizzare il processo di aggiornamento e patch management.

Prevenzione

Consapevolezza e formazione degli utenti

- Formare i dipendenti sui rischi delle reti Wi-Fi non sicure e su come riconoscere attacchi di phishing.
- Promuovere l’uso di VPN per connessioni remote sicure.

Segregazione della rete e controlli di accesso

- Segmentare la rete aziendale per limitare il movimento laterale di un potenziale attaccante.
- Implementare politiche di minimo privilegio per l’accesso ai dati e ai sistemi critici.

Aggiornamenti e patch

- Mantenere tutti i sistemi e software aggiornati con le ultime patch di sicurezza.
- Automatizzare il processo di aggiornamento e patch management.

Our Team

Simone La Porta

Team Leader

Nicolò Callegaro

Simone Esposito

Grazia Coco

Gianluca Sansone

Alejandro Cristino

Alessio Forli