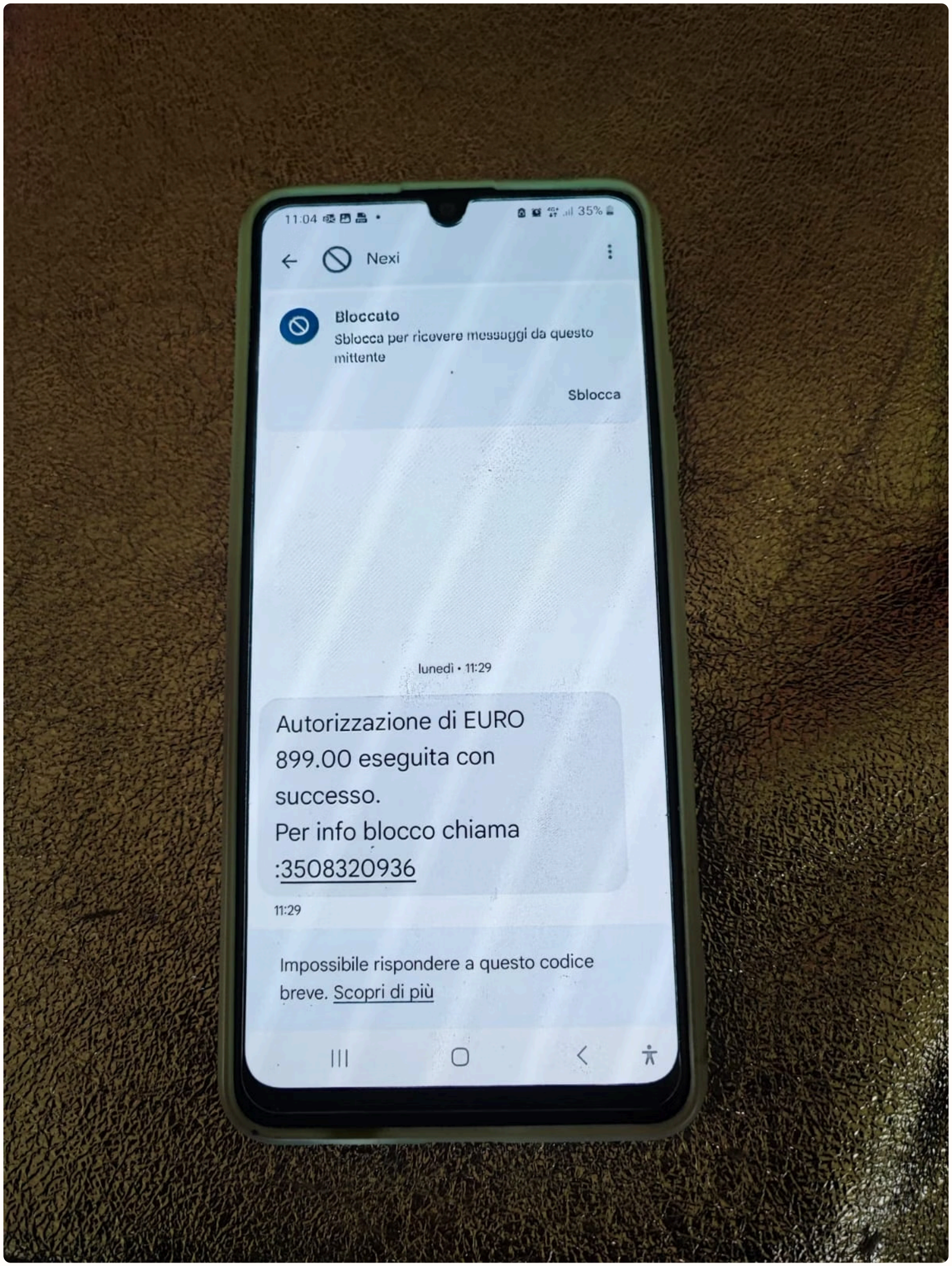
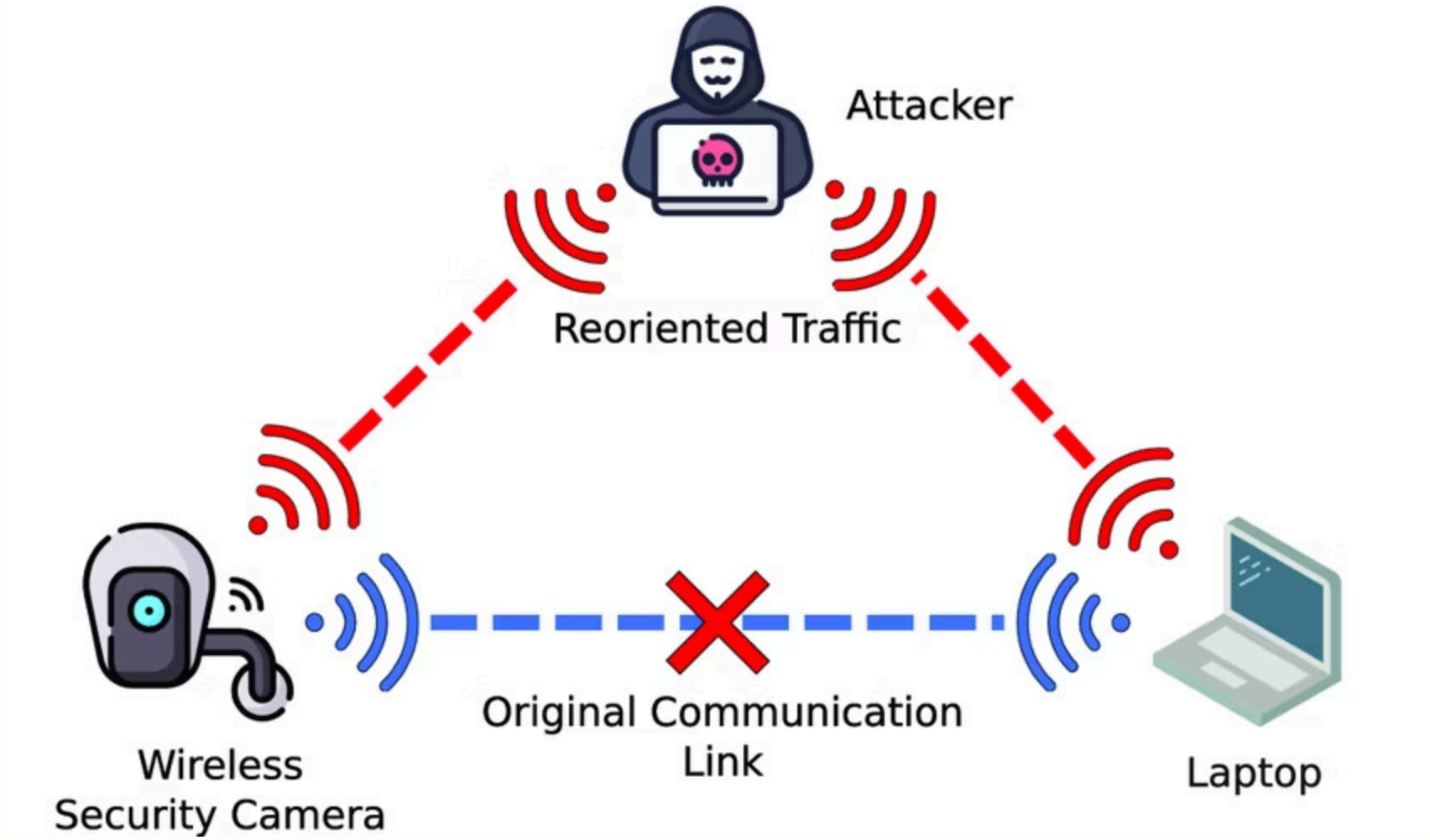
Tecniche di Spoofing: Una Panoramica Dettagliata

La parola **"spoofing"** deriva dall'inglese **"to spoof"**, che significa **"ingannare", "falsificare" o "simulare"**

Esploreremo diverse metodologie utilizzate dagli attaccanti per falsificare identità e manipolare sistemi di rete. Dallo spoofing TCP/IP all'IDN Homograph Attack, analizzeremo come queste tecniche vengono impiegate e quali contromisure possono essere adottate per proteggersi.

Prof. Demetrio Moschella


11:04
35%
Nexi
Bloccato
Sblocca per ricevere messaggi da questo mittente
Sblocca
lunedì • 11:29
Autorizzazione di EURO 899.00 eseguita con successo.
Per info blocco chiama :3508320936
11:29
Impossibile rispondere a questo codice breve. Scopri di più



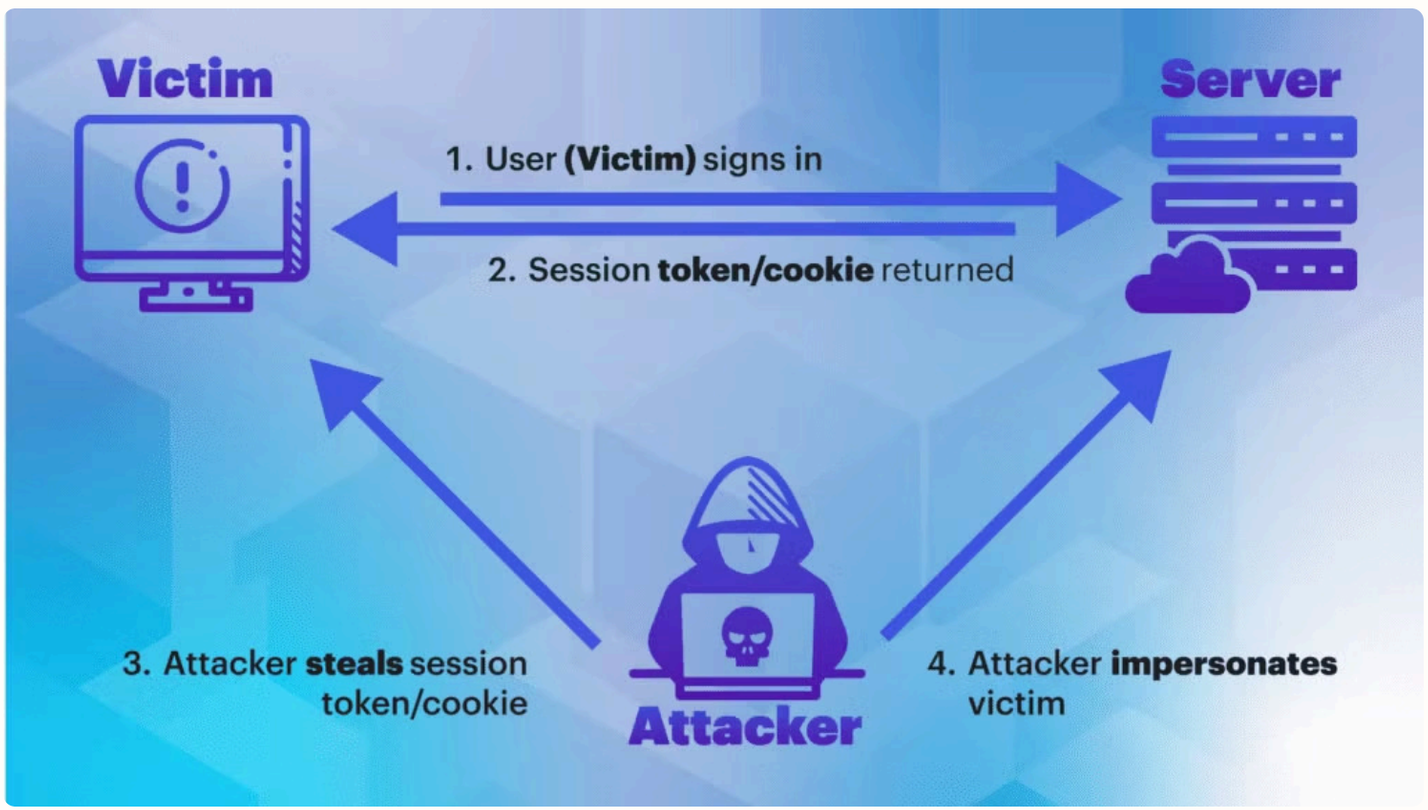
Man-in-the-Middle (MitM)

Intercettare e manipolare il traffico tra due parti.

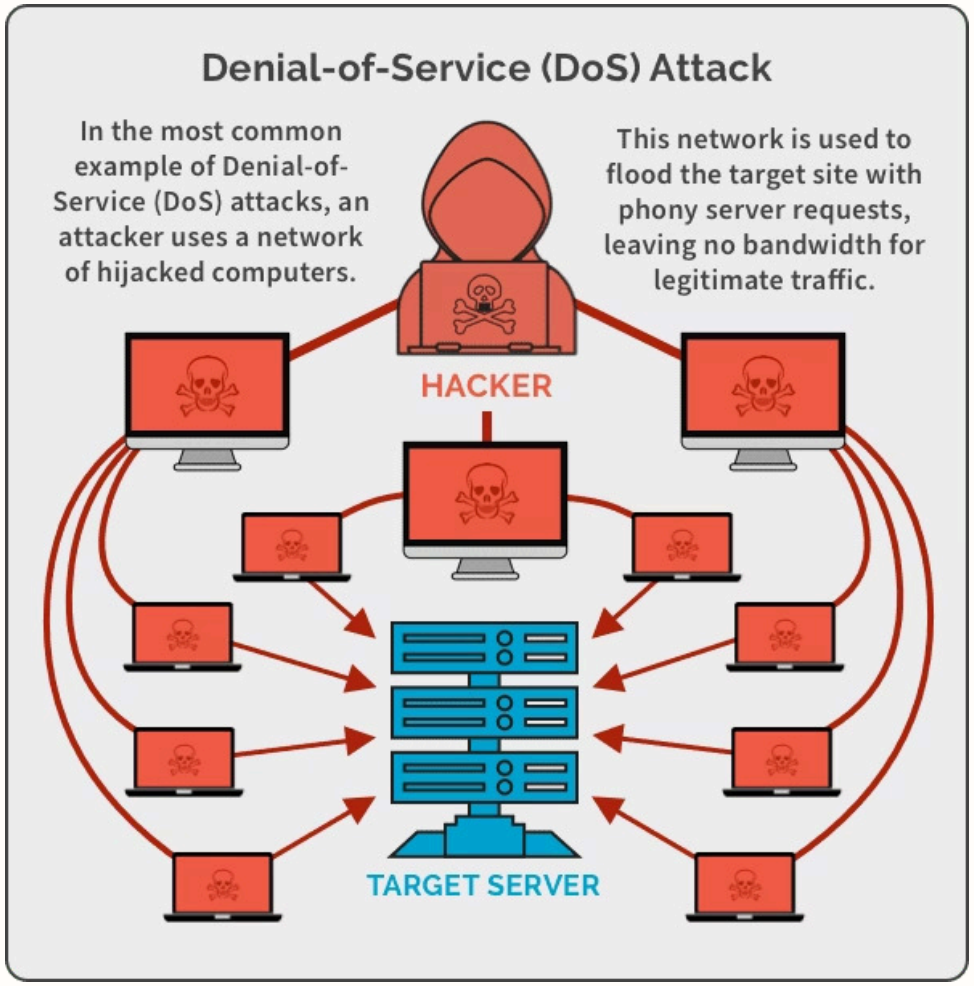
TCP/IP Spoofing: Falsificazione dell'Identità di Rete

Session Hijacking

Intercettare una connessione attiva per prendere il controllo della sessione.

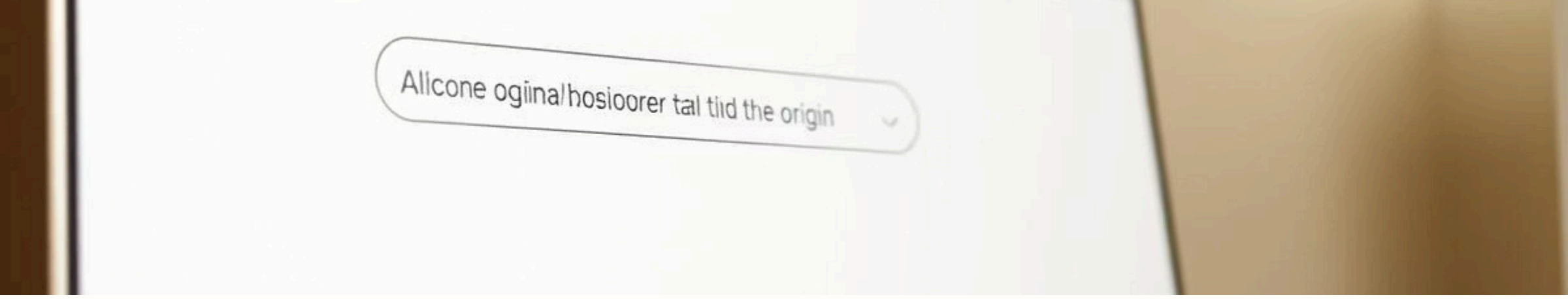


Il TCP/IP Spoofing è una tecnica in cui un attaccante falsifica l'indirizzo IP di origine nei pacchetti di rete, facendo credere al destinatario che la comunicazione provenga da una fonte legittima. Questo può essere usato per diversi attacchi.



Denial of Service (DoS)

Inondare un sistema da tantissimi dispositivi con pacchetti fasulli per renderlo inutilizzabile.



Referrer Spoofing: Manipolazione dell'Origine Web

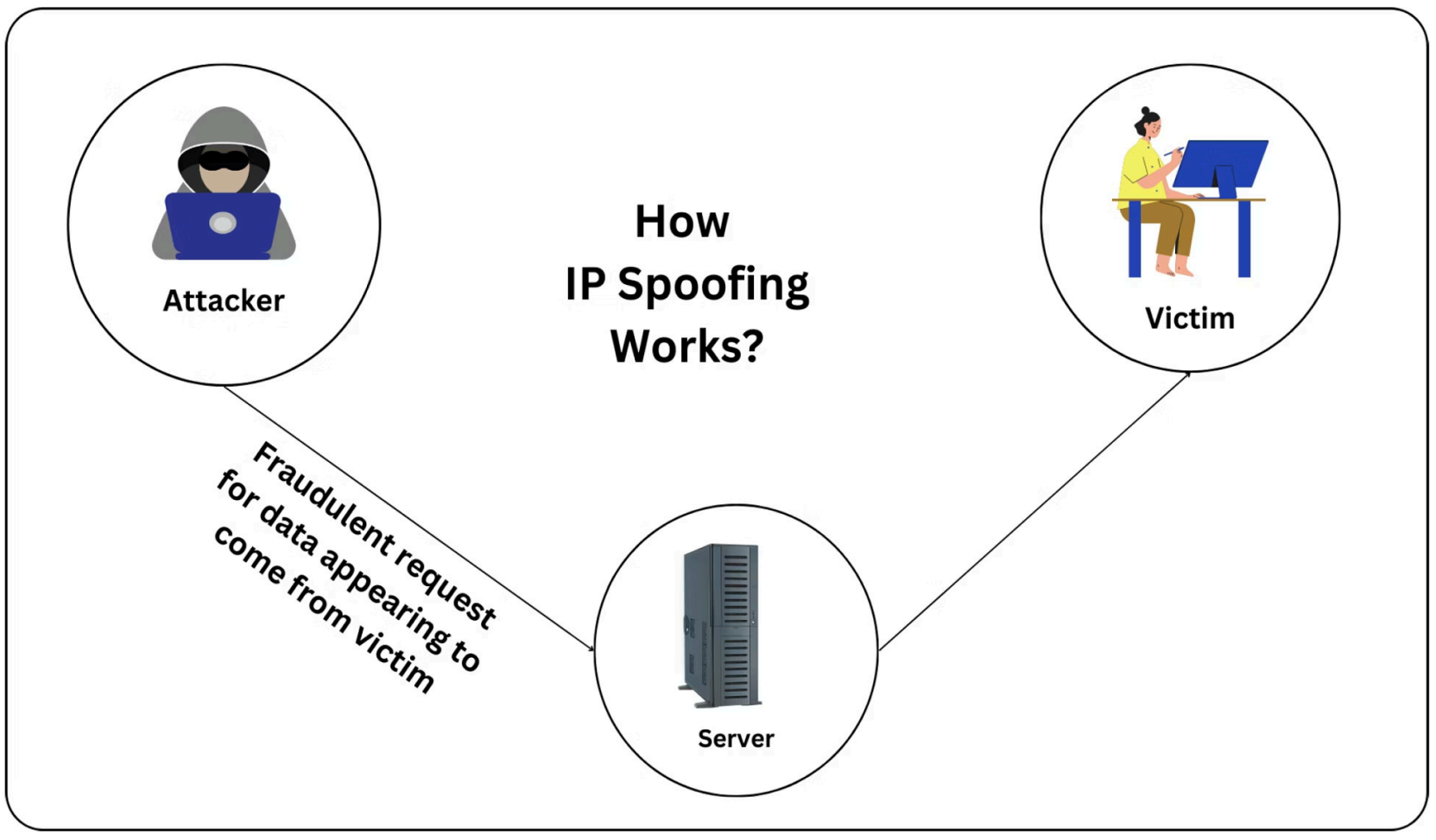
Evasione Restrizioni

Bypassare blocchi di contenuti basati sul referrer.

Tracciamento Fraudolento

Simulare visite da fonti specifiche per ingannare gli analytics.

Il Referrer Spoofing manipola l'intestazione HTTP "Referer" per nascondere o **falsificare l'origine di una richiesta web**. Questo viene spesso utilizzato per evadere restrizioni di accesso o per tracciamento fraudolento.



ARP e Link Spoofing: Intercettazione e Dirottamento

ARP Spoofing

Associare il proprio MAC address all'IP di un altro dispositivo.

Link Spoofing

Manipolare i link per reindirizzare a siti malevoli.

ARP Spoofing avviene quando un attaccante invia pacchetti ARP falsificati in una rete LAN per associare il proprio MAC address all'IP di un altro dispositivo. Link Spoofing manipola i link per indurre l'utente a cliccare su URL malevoli.

VoIP Spoofing: Falsificazione di Chiamate ed Email

Call Spoofing

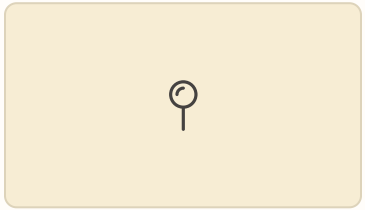
Alterare il numero di chiamata per truffe telefoniche.

Email Spoofing

Modificare l'indirizzo del mittente per phishing.

Il VoIP Spoofing comprende Call Spoofing, che altera il numero di chiamata, ed Email Spoofing, che modifica l'indirizzo del mittente. Entrambi sono usati per truffe e phishing.

Geo-location Spoofing: Falsificazione della Posizione GPS

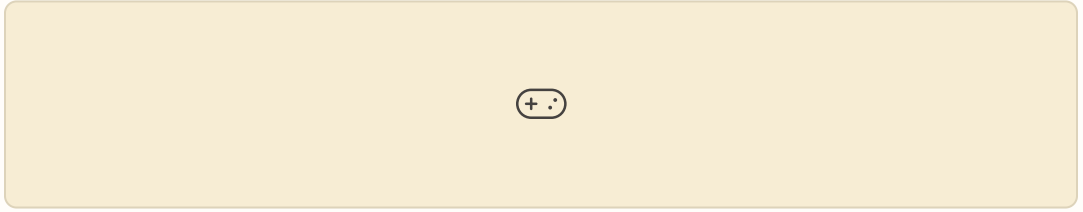


Accedere a contenuti

Con restrizioni geografiche.

Evitare la sorveglianza

Governativa o aziendale.



Barare nei giochi

Basati sulla posizione.

Lo spoofing della geolocalizzazione permette di falsificare la posizione GPS di un dispositivo. Viene utilizzato per accedere a contenuti con restrizioni geografiche, evitare la sorveglianza o barare nei giochi basati sulla posizione.

GPS e Pilot Spoofing: Manipolazione dei dati Gps

GPS

Manipolare i segnali GPS per far credere a un dispositivo di trovarsi in una posizione diversa.

Pilot

Simulare segnali radio per confondere piloti o sistemi di controllo del traffico aereo.

GPS Spoofing manipola i segnali GPS per alterare la posizione percepita di un dispositivo. Pilot Spoofing simula segnali radio per confondere piloti o sistemi di controllo del traffico aereo.

LAND Attack, DNS e MAC Spoofing: Tecniche di Interruzione

LAND Attack

Loop infinito consumando risorse di rete. È un tipo di attacco informatico in cui un pacchetto IP viene inviato con l'indirizzo del mittente e del destinatario uguale, causando un malfunzionamento nei sistemi che lo ricevono.

DNS Spoofing

Reindirizzare le richieste web a siti falsi.

MAC Spoofing

Impersonare un altro dispositivo per ottenere accesso.

Il LAND Attack è un DoS che causa un loop infinito. DNS Spoofing reindirizza le richieste web a siti falsi. MAC Spoofing impersona un altro dispositivo per ottenere accesso a reti protette.

IDN Homograph Attack: Cos’è e Come Funziona?

L’**IDN Homograph Attack** è un tipo di attacco di phishing in cui un hacker crea un sito web **visivamente identico** a uno reale, utilizzando caratteri simili provenienti da alfabeti diversi. Questo inganna gli utenti, facendoli credere di trovarsi su un sito affidabile, quando in realtà stanno visitando una **pagina malevola**.

- **IDN sta per Internationalized Domain Name**
- **Homograph significa "parola scritta in modo simile"**

Come funziona l’attacco?

L’attacco sfrutta le **somiglianze visive** tra alcuni caratteri dell’alfabeto latino e quelli di altri alfabeti, come il cirillico, il greco o altre lingue. Ad esempio:
✅ Il carattere latino **"a"** è diverso da quello cirillico **"а"**, ma visivamente sono quasi identici.
✅ La lettera latina **"o"** e la greca **"ο"** sono praticamente indistinguibili.

Un hacker può registrare un dominio con caratteri ingannevoli, come:

🔴 **"apple.com"**
🔴 **"google.com"**

(con "а" cirillica) anziché il vero "**apple.com**"
🔴 (con "ο" cirilliche) invece di "**google.com**"

Poiché i browser moderni supportano i **nomi di dominio internazionalizzati (IDN)**, un sito malevolo con questi caratteri può sembrare autentico nella barra degli indirizzi del browser.

Obiettivo dell’attacco

Il **principale scopo** dell’IDN Homograph Attack è:

- **Rubare credenziali di accesso**: L'utente inserisce username e password credendo di trovarsi sul sito originale.
- **Diffondere malware**: Il sito falso potrebbe scaricare virus o trojan.
- **Truffe finanziarie**: L'utente potrebbe inserire dati di pagamento su un sito fraudolento.

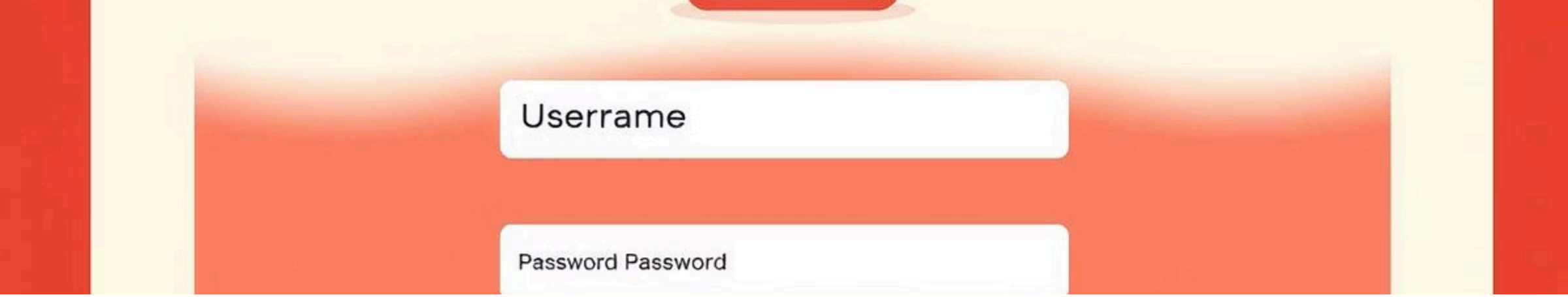
Esempio Pratico

Un utente riceve un’email che sembra provenire da "**paypal.com**", con un link che conduce a **link** (dove la "p" è cirillica). Il sito appare identico a PayPal e chiede di effettuare il login.
🚨 Se l’utente inserisce le proprie credenziali, queste vengono rubate dall'hacker.

Come Difendersi?

✅ **Attivare il controllo anti-phishing nei browser** (es. Google Chrome e Firefox bloccano i domini sospetti).
✅ **Passare il mouse sopra i link** per controllare la vera destinazione prima di cliccare.
✅ **Verificare il certificato SSL** (🔒 simbolo del lucchetto accanto all’URL).
✅ **Digitare manualmente l’indirizzo del sito** invece di cliccare su link sospetti.

💡 **Soluzione avanzata:** Alcuni browser moderni convertono automaticamente gli IDN sospetti in formato **Punycode** (es. **xn--unknown link**), rendendo più evidente il trucco.



Protocol e Website Spoofing, IDN Homograph Attack: Ulteriori Metodi di Inganno

Protocol Spoofing

Alterare protocolli di rete per intercettare o deviare il traffico.

Website Spoofing

Creare copie identiche di siti web per rubare credenziali.

IDN Homograph Attack

Sfruttare somiglianze tra caratteri per creare URL malevoli.

Protocol Spoofing altera i protocolli di rete. Website Spoofing crea copie di siti web per rubare credenziali. L'IDN Homograph Attack sfrutta somiglianze tra caratteri per creare URL che sembrano autentici ma conducono a siti malevoli.