Info Gathering

Il Google Hacking, noto anche come Google Dorking o Google Hacking Database (GHDB), è l'impiego di ricerche avanzate su motori di ricerca come Google per reperire informazioni specifiche su Internet che non sarebbero facilmente accessibili tramite ricerche standard.

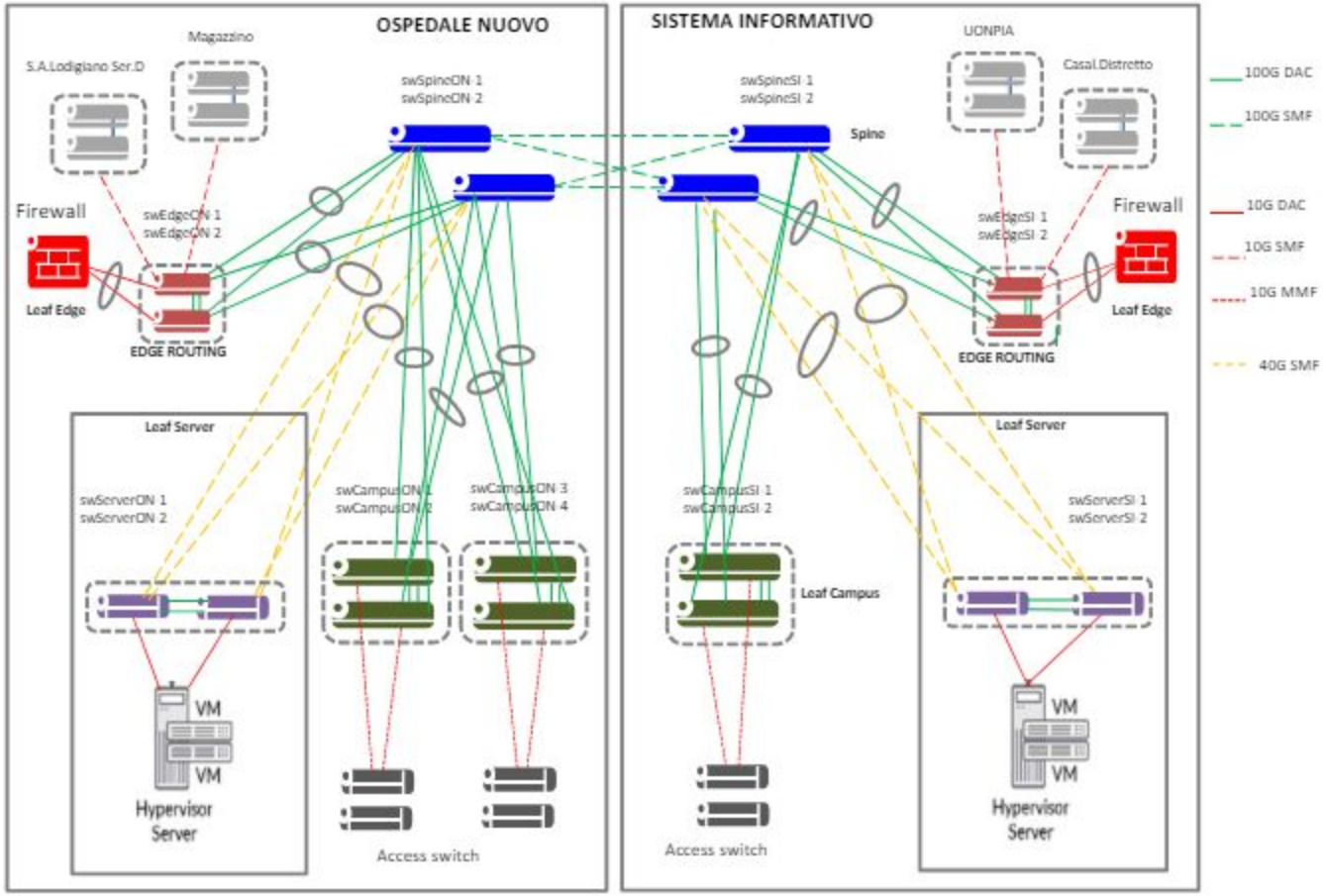
Definizione: Il Google Hacking è una tecnica che sfrutta le capacità avanzate di ricerca dei motori come Google per ottenere informazioni dettagliate e specifiche su Internet. Questo approccio consente agli utenti di scoprire dati nascosti o non facilmente individuabili tramite ricerche convenzionali, rendendolo un'utile risorsa per la sicurezza informatica e la ricerca di informazioni online.

Ecco una riscrittura migliorata del testo:

Per lo svolgimento di questo esercizio, è stato richiesto di condurre un'indagine utilizzando le query site, inurl, intext e filetype. I risultati hanno permesso di identificare le e-mail aziendali dei dipendenti, i curriculum dei dirigenti, i bandi contenenti dati sensibili delle aziende assegnatarie (come codice fiscale, numero di telefono ed e-mail), un documento PDF riguardante l'architettura del sistema di rete, i dispositivi utilizzati e la loro posizione fisica (una delle quattro immagini è allegata nella slide successiva).

Sulla base delle informazioni raccolte, è possibile progettare un phishing, un attacco fisico al sistema di sicurezza o tentare di sfruttare le vulnerabilità del sistema. Di fronte a questo scenario, le prime misure consigliate sono le seguenti:

1. Condurre una campagna di formazione sulla sicurezza informatica per sensibilizzare i dipendenti e permettere loro di riconoscere potenziali e-mail dannose, prevenendo così attacchi di ingegneria sociale.
2. Eliminare le informazioni online che potrebbero essere sfruttate da utenti malintenzionati, al fine di ridurre la superficie di attacco. La superficie di attacco rappresenta l'estensione totale utilizzabile da un malintenzionato per accedere ai sistemi interni e la sua riduzione contribuisce a rafforzare la sicurezza complessiva del sistema.



ARCHITETTURA SPB-M – 40G/100G

Di fianco il report come richiesto dall’esercizio Osint.

Sono stati raccolti i risultati dei dati ritrovati grazie ai tool: Google Hacking, TheHarvester e Maltego.

Nome	Versione / Querry	Scopo	Note
Google Hacking	site:	Limita la ricerca ai risultati provenienti solo dal dominio specifico	Rilevati cv dei dirigenti, titolari di incarichi
Google Hacking	inurl:	Ricerca specifiche pagine web all'interno del sito	Rilevata pagina di login rilevando il dominio dell'azienda
Google Hacking	intext:	Ricerca per pagine web in cui è presente il nome testuale dell'obiettivo	Rilevato un documento simile a ad una relazione Osint con indirizzo PEC per i protocolli
Google Hacking	filetype	Ricerca specifica del documenti e file pesenti sul sito	Rilevat PDF con schema dettagliato del sistema di rete
TheHarvester	nome dominio/all	Racolta di informazioni sul dominio come nomi host, indirizzi IP, dipendenti, indirizzi e-mail	Rilevati 6 indirizzi IP, 59 e-mail, 1 codice ASNS e 39 host
Maltego	Community Edition 4.3.0	Permette di esplorare connessioni, relazioni tra persone, organizzazioni, siti web, indirizzi email, nomi di dominio	Indivituata l'intera organizzazione di rete interna, con dispositivi, IPv4 e IPv6, Proxy e server