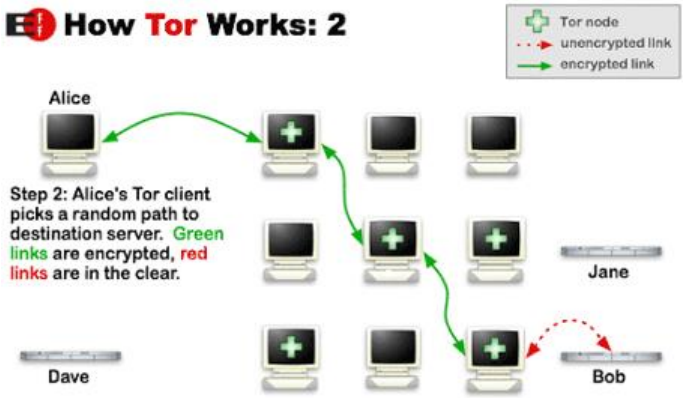
26/02 - Hacking e Sicurezza: Il Processo di Footprinting

TOR (*The Onion Ring*) è un sistema di comunicazione anonima che consente di navigare su Internet senza rivelare il proprio indirizzo IP. Per garantire l'anonimato, il traffico viene instradato attraverso diversi server distribuiti nel mondo e criptato più volte lungo il percorso. Questo processo, noto come onion routing, incapsula i dati in più livelli di crittografia, simili agli strati di una cipolla.

1. **Alice vuole navigare in modo anonimo** e utilizza il client Tor.
2. Per prima cosa, **ottiene una lista di nodi Tor da un server di directory** (indicato da Dave nella figura).
3. Questa lista contiene diversi **nodi Tor disponibili**, che saranno utilizzati per instradare il traffico.



1. **Alice seleziona casualmente un percorso** tra i nodi Tor per raggiungere il server di destinazione (Bob).
2. Il traffico passa attraverso **più nodi** per nascondere l'origine e proteggere l'anonimato.
3. **Le connessioni verdi** rappresentano i collegamenti crittografati, dove i dati sono protetti.
4. **L'ultimo tratto (linea rossa)** è non crittografato, perché il nodo di uscita deve inviare la richiesta al server di destinazione (Bob).

QUINDI:

- Alice non si connette direttamente a Bob, ma passa attraverso più nodi Tor.
- Ogni nodo sa solo da chi ha ricevuto i dati e a chi deve inviarli, ma **non conosce l'intero percorso**.
- Solo il nodo di uscita (ultimo nodo) invia i dati in chiaro a Bob, ma **non sa chi sia Alice**.

Questo metodo garantisce che nessun singolo nodo possa ricostruire l'intero percorso del traffico, **mantenendo l'anonimato dell'utente**.

FOOTPRINTING

Il footprinting è il processo sistematico e metodico di raccolta di informazioni su un'organizzazione per creare un profilo dettagliato del suo stato di sicurezza. Questa fase è essenziale per un attaccante, in quanto permette di ottenere dati critici su nomi di dominio, blocchi di rete, sottoreti, router, indirizzi IP e altri elementi chiave della sicurezza dell'infrastruttura bersaglio.

L'idea alla base del footprinting è quella di raccogliere il massimo numero di informazioni possibili prima di procedere con attacchi più invasivi. Esistono diverse tecniche di footprinting, che si concentrano principalmente su quattro ambienti:

1. **Internet** – Riguarda l'identificazione di nomi di dominio, blocchi di rete, indirizzi IP, servizi attivi, meccanismi di controllo degli accessi e sistemi di rilevamento delle intrusioni (IDS).
2. **Intranet** – Comprende l'analisi dei protocolli di rete interni, domini, indirizzi IP e sistemi di autenticazione.
3. **Accesso remoto** – Include la ricerca di numeri di telefono, sistemi di autenticazione e VPN.
4. **Extranet** – Si focalizza sulla natura delle connessioni tra partner esterni e l'organizzazione bersaglio.

Importanza del Footprinting

Il footprinting consente di determinare quali informazioni siano accessibili a un potenziale attaccante, evidenziando così le vulnerabilità esposte. Conoscendo questi dettagli, un'organizzazione può anticipare eventuali minacce e implementare contromisure adeguate.

Metodologia

Gli hacker utilizzano una combinazione di strumenti e tecniche, insieme a un'analisi metodica e paziente, per raccogliere dati. Questo processo può avvenire in modo **passivo**, attraverso la ricerca di informazioni pubbliche senza interagire direttamente con il bersaglio, o in modo **attivo**, tramite richieste dirette a server, DNS e altri servizi.

Le Fasi del Footprinting

Il processo di footprinting si suddivide in più fasi, che comprendono la definizione dell'ambito di analisi, la raccolta di informazioni pubblicamente disponibili, l'enumerazione di database WHOIS e DNS, e l'analisi dell'infrastruttura di rete.

1. Determine the scope of your activities

Il primo passo è stabilire chiaramente l'ambito dell'analisi di footprinting. Questo include la determinazione delle aree da esaminare, come l'intera organizzazione, partner commerciali o siti di disaster recovery. È cruciale individuare tutte le potenziali vulnerabilità per non lasciare spazi di attacco agli hacker.

2. ***Get proper authorization***

Considerare gli aspetti politici e finanziari (livelli 8 e 9 del modello OSI) è essenziale nei test di penetrazione. Prima di iniziare qualsiasi attività, occorre ottenere un'autorizzazione chiara, verificare che provenga dalla persona giusta e preferibilmente averla in forma scritta. È fondamentale accertarsi che gli indirizzi IP e gli obiettivi siano corretti. La "carta per uscire di prigione" rappresenta una tutela legale per gli ethical hacker. Sebbene il footprinting richieda discrezione, è sempre consigliabile informare i superiori prima di procedere.

3. ***Publicly available information***

Molte informazioni sensibili possono essere raccolte da pagine web aziendali senza necessità di accesso diretto ai sistemi interni.

3.1 Company Web Pages

1. **Analisi delle Pagine Web**

   Codice sorgente HTML: commenti nascosti, percorsi interni, credenziali hardcoded.

   Strumenti per il mirroring: Wget (Linux), Teleport Pro (Windows).

2. **Scansione di File e Directory Nascoste**

   OWASP DirBuster per enumerare directory e file non documentati.

   Proxying tramite Privoxy per anonimizzare le richieste ed evitare rilevamenti.

3. **Accesso a Risorse Interne via Web**

   Proxy verso server interni, come Microsoft Exchange, per intercettare comunicazioni.

4. **Siti Correlati e Secondari**

   Sottodomini e ambienti di test: www1, test, vpn, dev.

   Organizzazioni collegate: partner o filiali possono esporre dati sensibili.

3.2 Related Organizations Location Details

1. **Rischi dell'Esternalizzazione dello Sviluppo Web**

   Partner poco attenti alla sicurezza possono esporre dati critici.

   Ingegneria sociale sfruttando aziende terze con minori controlli.

2. **Geolocalizzazione e Sorveglianza**

   Dumpster-diving, accesso fisico non autorizzato e social engineering.

   Google Earth, Maps e Street View per analizzare sedi aziendali e accessi.

   Geolocalizzazione Wi-Fi tramite MAC address (Skyhook, Google Location Services).

3. **Caso di Studio: BlackHat 2010**

   La demo *"How I Met Your Girlfriend"* ha mostrato come tracciare la posizione di dispositivi tramite MAC address, evidenziando i rischi legati alla raccolta di dati pubblici.

3.3 Employee Information

1. **Dati Personali e Professionali**

   Nomi → Email e username utilizzabili per attacchi mirati.

   Numeri di telefono → Indirizzi fisici (tramite servizi come Phonenumber.com, 411.com, Yellowpages.com).

   Altri dettagli personali reperibili su Blackbookonline.info, Peoplesearch.com.

   Dati sensibili: indirizzi di casa, numeri di previdenza sociale, storico creditizio e casellari giudiziari ottenibili da social network, siti di genealogia e piattaforme di condivisione foto.

2. **Fonti di Informazioni Pubbliche**

   Social e professional network: Facebook, LinkedIn, Twitter, MySpace, Plaxo, Classmates, Reunion.

   Siti di ricerca lavoro: Monster.com, Careerbuilder.com, Dice.com.

   Servizi di directory aziendali: JigSaw.com, usato dai team di vendita per raccogliere contatti (incentivi per aggiornare voci).

3. **Annunci di Lavoro e Curriculum**

   Informazioni tecniche involontariamente esposte: "Checkpoint firewalls e Snort IDS" nei CV indicano le tecnologie aziendali.

   Google Hacking: cercare “company resume firewall” per trovare CV di attuali ed ex dipendenti.

   Job sites: monitorare annunci su Monster.com, Careerbuilder.com.

   Ex-dipendenti scontenti: rischio di fughe di dati per vendetta.

4. **Rischi Legati ai Computer Personali dei Dipendenti**

   Accesso remoto ai sistemi aziendali attraverso dispositivi domestici.

   Keylogger e malware per compromettere credenziali.

   Impersonificazione di utenti fidati per accesso fraudolento ai sistemi aziendali.

3.4 Publicly Available Information Current Events

Eventi come **fusioni, acquisizioni, scandali, licenziamenti, assunzioni rapide e riorganizzazioni** possono creare vulnerabilità:

Fusioni/acquisizioni: integrazione delle reti con sicurezza ridotta.

Fattore umano: dipendenti demotivati aggiornano il CV o favoriscono accessi non autorizzati.

SEC (Securities and Exchange Commission): report 10-Q e 10-K su *sec.gov* rivelano organigrammi aziendali.

Fonti finanziarie: *Yahoo! Finance* e forum di trading offrono insight su strategie e crisi aziendali.

3.5 Privacy or Security Policies, Archived Information

Privacy e security policies: possono rivelare dettagli tecnici sui meccanismi di sicurezza adottati.

Informazioni archiviate: versioni precedenti di documenti spesso contengono più dettagli delle versioni attuali.

- **Fonti**: *Archive.org* e cache di *Google*.

3.6 Search Engines and Data Relationships

Motori di ricerca: Google, Bing, Yahoo, Dogpile, Ask.

Tecniche di ricerca usate dagli hacker: Google Hacking Database (GHDB) su hackersforcharity.org/ghdb/.

Ricerca nella cache di Google per vulnerabilità, errori e problemi di configurazione.

- *Strumenti*: Athena (snakeoillabs.com), SiteDigger (foundstone.com), Wikto (sensepost.com/research/wikto).

Analisi dei metadati nei file web: per rilevare perdite di informazioni (es. FOCA su informatica64.com).

Mining e collegamento di informazioni rilevanti: strumento Maltego (paterva.com).

3.7 Contromisure alla sicurezza delle banche dati pubbliche:

Site Security Handbook: RFC 2196.

Rivedere periodicamente e rimuovere dati sensibili pubblici.

4. WHOIS e DNS Enumeration

In questa fase, vengono raccolti dati da fonti pubbliche come WHOIS, che forniscono informazioni sui domini registrati, i loro proprietari, i contatti amministrativi e gli indirizzi IP associati. WHOIS è gestito da ICANN e archiviato in server WHOIS/DNS. I dati sono organizzati in tre categorie: registry (gestore del dominio), registrar (l'ente che registra i domini) e registrant (il proprietario del dominio).

Per esempio, se si vuole cercare keyhole.com, si inizia con whois.iana.org per trovare il registry e il registrar. Strumenti automatici come whois, allwhois e superscan aiutano a fare queste ricerche velocemente.

Inoltre, l'enumerazione DNS permette di raccogliere informazioni sui server di dominio, rivelando la struttura di rete e possibili errori di configurazione. Un errore comune è permettere a persone non autorizzate di trasferire zone DNS, esponendo la rete interna dell'organizzazione.

Quando si cercano indirizzi IP, come 61.0.0.2, si parte da arin.net e si continua su altri siti per scoprire chi gestisce quel dato IP. Tuttavia, bisogna tenere a mente che gli indirizzi IP potrebbero essere falsificati.

5. DNS interrogation

Si analizza il DNS alla ricerca di configurazioni vulnerabili, come trasferimenti di zona aperti, che potrebbero esporre dettagli interni dell'infrastruttura. Interrogare i server DNS permette di ottenere informazioni sui record associati a un dominio, come:

5.1 Raccolta di Informazioni tramite DNS

Query ai server DNS per ottenere dettagli su domini e IP.

1. **Zone transfer non autorizzati**:

   Possibili per configurazioni errate.

   Trasferimento da server primario a secondario può rivelare **host interni e IP privati**.

   Strumento: dnsrecon.

2. **Raccolta di record DNS** con nslookup:

   Tipi di record: A, RP, MX, HINFO, ecc.

   HINFO: informazioni sull'host (potenzialmente pericolose se esposte).

   Strumenti avanzati: dnsenum, dnsmap, fierce, host.

   Analisi con: grep, sed, awk, perl.

5.2 Contromisure di Sicurezza DNS

Limitare il zone transfer solo ai server autorizzati (*named.conf* in BIND).

Bloccare connessioni non autorizzate alla porta TCP 53 tramite firewall.

Evitare l'esposizione di informazioni interne nei record DNS.

Eliminare i record HINFO per prevenire la divulgazione di dettagli sugli host.

6. Network reconnaissance

Il passo finale del **footprinting** riguarda l'analisi della struttura di rete di un bersaglio. Tecniche come il **traceroute** consentono di identificare il percorso seguito dai pacchetti dati per raggiungere una destinazione, rivelando dettagli sui **router e firewall intermedi**.

6.1 Strumenti per l'Analisi del Percorso di Rete

Traceroute, tracert, visualroute, NeoTrace (McAfee), Trout (Foundstone) per tracciare il percorso dei pacchetti.

Informazioni raccolte:

- Identificazione dei nodi intermedi (router, firewall, gateway).
- Analisi dei **Time-To-Live (TTL)** e pacchetti **ICMP** per rilevare la struttura della rete.

6.2 Contromisure contro la Ricognizione di Rete

Sistemi di rilevamento intrusioni: *Snort*, *Bro* per monitorare attività sospette.

Configurazione di sicurezza per i router di frontiera:

- Limitare traffico **ICMP** e **UDP** solo ai sistemi autorizzati per impedire la scansione di rete.