A.A. 2023/24

Samba Deception Component Generator

Progetto di Cybersecurity M

Autori

Cassanelli Antonio

Focardi Leonardo

Galeone Christian

Sommario

Introduzione

L'importanza dei metodi di deception nel campo della cyber security si manifesta come un **elemento cruciale** nella sfida in costante evoluzione contro le minacce informatiche. In un panorama digitale sempre più complesso e pericoloso, gli esperti di sicurezza informatica sono chiamati a implementare strategie avanzate per proteggere le reti, i sistemi e i dati sensibili. I metodi di deception, o "trappole" digitali, emergono come una tattica fondamentale per ingannare e scoraggiare gli attaccanti, offrendo un approccio proattivo alla cyber defence.

Questi metodi si basano sulla creazione di elementi fittizi all'interno di un ambiente di rete, progettati per simulare risorse e informazioni allettanti per gli aggressori. Attraverso l'uso di trappole come documenti, credenziali o server fasulli, le organizzazioni possono confondere e rallentare gli attaccanti, consentendo nel frattempo di rilevare e rispondere prontamente agli attacchi in corso. Questa forma di "inganno intelligente" non solo protegge le risorse reali, ma fornisce anche agli esperti di sicurezza preziose informazioni sulla metodologia degli attaccanti e sulle nuove minacce emergenti.

In un contesto in cui la sofisticazione delle minacce informatiche è in costante crescita, l'adozione di metodi di deception si rivela essenziale per rafforzare la postura di sicurezza di un'organizzazione. Questa strategia, integrata con altre misure di sicurezza, contribuisce a creare un ambiente più ostile per gli aggressori, riducendo la probabilità di successo degli attacchi e migliorando complessivamente la resistenza del sistema alle minacce informatiche. In un panorama in continua evoluzione, l'utilizzo intelligente dei metodi di deception si conferma, dunque, come un elemento chiave nella difesa proattiva delle risorse digitali.

Tecnologie

Samba

Samba è una suite di software open source progettata per consentire la condivisione di file e stampanti tra sistemi operativi diversi all'interno di una rete. La sua funzione principale è agevolare l'interoperabilità tra ambienti basati su Linux/Unix e Windows, utilizzando il protocollo SMB/CIFS. Samba gestisce l'autenticazione degli utenti, facilita la condivisione di risorse e può fungere da controller di dominio in reti Windows, consentendo una collaborazione fluida tra sistemi eterogenei. Grazie alla sua flessibilità, Samba è ampiamente adottato sia in ambienti aziendali che domestici.

A partire da Samba 4, è stato incorporato un server LDAP interno, semplificando la gestione delle directory direttamente attraverso Samba. Prima di questa versione, era comune l'uso di server LDAP esterni. Questa integrazione offre una maggiore facilità di configurazione e gestione, consentendo a Samba 4 di operare autonomamente come controller di dominio completo, compresa la gestione delle informazioni di directory attraverso il suo server LDAP integrato. [1]

LDAP

LDAP (*Lightweight Directory Access Protocol*) è un protocollo di rete specializzato per la gestione di directory distribuite. Organizza le informazioni gerarchicamente, facilitando la ricerca e l'accesso a dati strutturati. Opera su un modello client-server, consentendo la richiesta di informazioni da parte di un client a un server. LDAP è noto per la sua efficienza nelle ricerche, la portabilità su diverse piattaforme e il supporto per la sicurezza, inclusi meccanismi di autenticazione e crittografia. Comunemente impiegato per la gestione delle identità e degli accessi in ambienti aziendali, offre una solida base per la memorizzazione e il recupero di informazioni come dettagli sugli utenti, gruppi e risorse di rete. [2]

Python

Python è un linguaggio di programmazione ad alto livello, interpretato e versatile. Notato per la sua sintassi chiara e leggibile, è adatto a principianti e esperti. Supporta vari paradigmi di

programmazione e dispone di una vasta libreria standard per facilitare lo sviluppo. La comunità di sviluppatori è attiva, offrendo supporto e risorse. Python è cross-platform e utilizzato in diversi settori, come sviluppo web, data science e intelligenza artificiale. La sua versatilità lo rende uno dei linguaggi più popolari. [3]

Docker

Docker è una piattaforma open-source che semplifica il deployment e la gestione di applicazioni utilizzando container leggeri. I container contengono tutto ciò che serve per eseguire un'applicazione, rendendo facile il trasferimento tra diversi ambienti senza preoccuparsi delle differenze di configurazione. Gli sviluppatori definiscono le applicazioni e le loro dipendenze attraverso Dockerfile, creano immagini Docker e le distribuiscono tramite registri come Docker Hub. Docker promuove la portabilità, l'isolamento e la scalabilità delle applicazioni, rendendo più efficiente il ciclo di sviluppo e deployment. [4]

Ubuntu

Ubuntu è un sistema operativo basato su Linux, noto per la sua stabilità, affidabilità e facilità d'uso. È una distribuzione gratuita e open source che deriva da Debian e è sviluppata dalla società Canonical Ltd. Ubuntu è ampiamente utilizzato sia come sistema operativo desktop che come sistema server.
L'immagine di Ubuntu per Docker offre un ambiente Linux leggero e isolato che può essere eseguito su qualsiasi host Docker compatibile. [5]

Pandoc

Pandoc è uno strumento open-source scritto in Haskell per la conversione di documenti tra diversi formati. Supporta input e output in numerosi formati, tra cui Markdown, HTML, LaTeX e PDF. La sua flessibilità consente la gestione di documenti complessi e offre estensibilità attraverso un sistema di estensioni. Pandoc è ampiamente utilizzato per facilitare la conversione di documenti mantenendo una formattazione coerente, rendendolo popolare tra scrittori, ricercatori e sviluppatori. [6]

Kerberos

Kerberos è un protocollo di autenticazione di rete che garantisce un accesso sicuro verificando l'identità degli utenti tramite token di autenticazione. Samba può utilizzare Kerberos per fornire un accesso sicuro alle risorse di rete. Quando integrato con Kerberos, Samba emette e verifica biglietti di autenticazione, consentendo agli utenti di accedere alle risorse in modo sicuro senza dover autenticarsi ad ogni richiesta.
L'uso di Kerberos migliora la sicurezza del sistema, prevenendo attacchi come il furto di credenziali. La configurazione di Samba con Kerberos richiede l'integrazione con un sistema Kerberos locale o di dominio. [7]

Progetto

Implementazione

L'intero progetto si fonda su uno script Python che consente di selezionare le personalizzazioni desiderate per l'implementazione del container Samba. In particolare, permette di:

- Abilitare condivisioni pubbliche e/o private
- Creare un file system gerarchico popolato con file pdf e word
- Abilitare l'autenticazione LDAP
- Creazione di utenti e gruppi locali
- Build e run dell'immagine all'interno dello script (se non viene scelta l'autenticazione con LDAP)
- Cancellazione dei file creati

Lo script genera tre file (`Dockerfile`, `setup.py` e `start.sh`) personalizzati in base alle preferenze dell'utente. Ogni file verrà analizzato nel dettaglio successivamente.

Setup.py

Questo file ha il compito di creare il supporto all'interno del sistema per il server. In particolare, è responsabile della creazione degli utenti e dei gruppi, modificando opportunamente il file system in base alla scelta di condivisione effettuata dall'utente. Il file fa ampio uso del modulo subprocess, il quale consente l'esecuzione di comandi bash attraverso Python.

Nel caso in cui l'utente abbia scelto l'autenticazione LDAP, il presente file assume la responsabilità di creare l'intero sottoalbero di autenticazione all'interno del sistema. La funzione `setup_ldap(domain, adminpasswd)` è incaricata di generare i file di Kerberos, creare i domini tramite samba-tool e modificare la password dell'amministratore con quella scelta dall'utente.

Per l'autenticazione LDAP, è necessario creare gli utenti attraverso samba-tool. Questo compito è affidato alla funzione denominata `create_user`, illustrata di seguito. Successivamente, è indispensabile inizializzare gli utenti in Kerberos mediante la funzione `kinit_user(username, password)`.

La funzione `create_user(username,password)` a seconda della scelta dell'utente può generare l'utente LDAP tramite samba-tools, oppure lo genera sia all'interno del sistema sia come utente Samba standard; inoltre la funzione create_group(group_name, list), crea il gruppo con il nome specificato aggiungendogli tutti gli utenti specificati all'interno di group_list, genera anche una cartella condivisa tra gli utenti del gruppo.

Le password vengono inserite all'interno del file in chiaro. Questa scelta, sebbene non sia completamente in linea con i principi della programmazione sicura, è giustificata dal fatto che, all'interno del container, le password sono memorizzate in forma cifrata. Inoltre, il file `setup.py` viene rimosso dal container una volta completata la fase di configurazione. Questa decisione agevola la possibilità di apportare modifiche future agli utenti e alle password direttamente attraverso la modifica del file, in modo da generare altre immagini Docker con credenziali differenti, senza la necessità di ricorrere allo script principale.

La funzione `makeFS(type)` genera il file system, se type è:

- **Public**: viene generata la cartella omonima con all'interno due sottocartelle `Shared_Documents` e `Shared_Images`
- **Private**: per ogni utente viene generata la cartella personale denominata con lo stesso nome dell'utente, all'interno della quale vengono create le seguenti sottocartelle
    - `Documents`
    - `Documents/personal/`
    - `Documents/personal/lawyer`
    - `Documents/personal/family`, `Documents/work/`

    - Documents/work/projects
    - Pictures
    - Downloads
    - Downloads/important_documents
    - Desktop
    - Desktop/trash
    - Desktop/work
- **Both**: genera il file system sia per la cartella pubblica sia per cartelle private

Per ogni cartella generata, vengono modificati i permessi in modo da consentire l'accesso agli utenti e i gruppi specificati; inoltre, viene creato un numero casuale di file di testo compreso tra 5 e 15, i quali vengono successivamente convertiti in formato PDF e Word attraverso Pandoc. In seguito, i file di testo vengono eliminati.

La generazione dei file di testo avviene tramite funzione `create_files(dim_min,dim_max,num_file)` che crea `num_file` file di nome casuale nel formato `<nome_casuale>_<data_casuale>.txt`; ogni file è popolato da parole casuali separate da segni di punteggiatura.

Il file viene modificato dallo script principale aggiungendo alla fine le chiamate alle funzioni descritte in precedenza.

Start.sh

Questo è il file eseguito all'interno del container per avviare i servizi. Sono disponibili due versioni: nel caso di utilizzo di LDAP, il file modifica /etc/resolv.conf per adattare il DNS di sistema e avvia il servizio samba-ad-dc; nel caso di utilizzo di Samba tradizionale, avvia il servizio smbd.

Dockerfile

Il Dockerfile ha il compito di creare l'immagine del server Samba. Utilizzando come base l'immagine di Ubuntu 20.04, si procede all'installazione dei pacchetti necessari per configurare l'intero sistema. Successivamente, il file di configurazione denominato setup.py viene copiato, eseguito e rimosso. Per ridurre l'ingombro, vengono eliminati tutti i pacchetti di Pandoc, ormai

superflui. Successivamente, il file start.sh viene copiato all'interno del container, vengono esposte le porte necessarie, ed viene eseguito lo script di avvio.

Utilizzo del generatore

1. Clona il repository da Github:
   `git clone https://github.com/LEOB3TA/Samba-deception-component-generator`
2. Entra nella directory `Samba-deception-component-generator`
   `cd Samba-deception-component-generator`
3. Installa i requisiti:
   `pip install -r requirements.txt`
4. Esegui il file `samba_deception_component_generator.py`
   `python3 samba_deception_component_generator.py`

Una volta eseguito il file, verrà mostrata una CLI (Command Line Interface) per scegliere tutte le opzioni descritte in precedenza. Alla fine dell'esecuzione i file generati saranno creati all'interno della cartella `image`.

Utilità di Samba Deception Component

L'implementazione di un componente di deception in un ambiente basato su Samba è cruciale per la sicurezza informatica. Fornisce una difesa proattiva rilevando minacce in modo precoce, riducendo falsi positivi, analizzando il comportamento degli attaccanti e rallentando la progressione degli attacchi. Contribuisce a proteggere risorse critiche e offre un vantaggio tattico nella lotta contro le minacce cibernetiche.

In particolare, il protocollo SMB, quando non si appoggia a LDAP per l'autenticazione, utilizza un protocollo di autenticazione di Windows noto come NTLM (NT Lan Manager) o NTLMv2. Entrambi i protocolli sono considerati vulnerabili a causa della debolezza degli algoritmi di hash utilizzati. In particolare, NTLM fa uso dell'algoritmo di hash MD4, mentre NTLMv2 fa uso di HMAC-MD5. Questa scelta rende entrambi gli algoritmi vulnerabili agli attacchi di forza bruta.
Inoltre tali protocolli sono vulnerabili a:

- **Pass-the-Hash Attacks**: entrambi gli algoritmi NTLM e NTLMv2 sono soggetti a attacchi "pass-the-hash". In questi attacchi, un aggressore può utilizzare l'hash della password rubata anziché la password stessa per autenticarsi, bypassando così la necessità di conoscere la password effettiva.
- **Man-in-the-Middle Attacks**: NTLM è intrinsecamente più vulnerabile a attacchi Man-in-the-Middle (MITM) rispetto a protocolli di autenticazione più sicuri come Kerberos. Un attaccante potrebbe intercettare e manipolare le comunicazioni SMB che utilizzano NTLM, compromettendo così la sicurezza dell'autenticazione.
- **Sicurezza dei Protocolli Legacy**: poiché SMB1 (la versione più vecchia di SMB) è spesso configurato per utilizzare NTLM, i sistemi che eseguono versioni più datate di SMB sono esposti a vulnerabilità di sicurezza note associate all'uso di NTLM.
- **Esposizione delle Credenziali**: In un ambiente in cui NTLM o NTLMv2 sono utilizzati senza crittografia o con crittografia debole, le credenziali degli utenti possono essere esposte durante il processo di autenticazione, rendendole vulnerabili a intercettazioni non autorizzate. [1]

Nel caso in cui si faccia affidamento su un server LDAP, le vulnerabilità precedentemente descritte sembrano attenuarsi. Tuttavia, escludendo le vulnerabilità intrinseche al server LDAP, ne emerge un'altra altrettanto critica. In particolare, su un controller di dominio Samba 4, il server LDAP, in tutte le versioni di Samba dalla 4.0.0 in poi, valida erroneamente i permessi per la modifica delle password tramite LDAP. Tale falla consente agli utenti autenticati di modificare le password di qualsiasi altro utente, inclusi gli utenti amministrativi e gli account di servizio privilegiati. [2]
Questo difetto apre la strada a possibili sfruttamenti da parte di utenti malintenzionati, permettendo loro di compromettere le credenziali di altri utenti, incluso l'accesso a account con privilegi elevati come quelli degli amministratori di sistema o degli account di servizio critici.

Un’altra vulnerabilità molto importante riguarda un problema di sicurezza nel tool di amministrazione Samba AD DC (Active Directory Domain Controller), noto come samba-tool, che invia le password in chiaro quando opera con un server LDAP remoto. Questo problema colpisce tutte le versioni di Samba dalla 4.0 in poi.
In breve, quando samba-tool opera con un server LDAP remoto, invia le nuove o reimpostate password su una connessione firmata di default. Tuttavia, Active Directory richiede che queste

operazioni avvengano solo su una connessione crittografata, una restrizione che Samba attualmente non implementa. [3]
Questo comporta un rischio di sicurezza, poiché un attaccante che può osservare il traffico di rete tra samba-tool e il Samba AD DC potrebbe ottenere le password appena impostate se samba-tool si connette utilizzando una connessione LDAP.
Nel nostro caso questa vulnerabilità non sussiste in quanto, il server LDAP utilizzato è quello interno a SAMBA stesso.

Inoltre, poichè Samba AD DC utilizza Kerberos potrebbe essere vulnerabile agli attacchi:

- **Attacchi "pass-the-ticket"** (passaggio del biglietto), in cui i malintenzionati intercettano e riutilizzano i biglietti inviati a o da un utente autenticato.
- **Attacchi "golden ticket"**, noti anche come attacchi "DC shadow", in cui i malintenzionati ottengono l'accesso necessario per creare il proprio controllore di dominio in Windows. In questo modo possono creare credenziali con privilegi fasulle che garantiscono loro un accesso illimitato alle risorse di rete.
- **Attacchi di furto di credenziali**, in cui i malintenzionati tentano di compromettere le password degli utenti. Questi attacchi sono generalmente rivolti ai server di autenticazione KDC o ai servizi di concessione dei biglietti.

Tuttavia, anche se nessuna tecnologia è completamente inattaccabile, Kerberos è abbastanza sicuro se configurato e gestito correttamente. [4]

Un server Samba non costituisce intrinsecamente una minaccia, poiché un potenziale attaccante può solamente leggere i dati presenti al suo interno. Tuttavia, la reale preoccupazione sorge nel caso in cui l'attaccante riesca ad acquisire l'hash di un utente configurato nell'Active Directory. In tale circostanza, si apre la possibilità di ottenere accesso all'intero dominio associato a detto utente.

Date queste premesse, emerge chiaramente che il componente di deception costituisce un autentico honeypot per gli attaccanti del sistema. Questa implementazione consente di deviare gli aggressori dai veri obiettivi, creando una sorta di trappola virtuale che attira l'attenzione e le risorse degli attaccanti lontano dai punti critici del sistema.

Attraverso l'analisi dei log generati da questo honeypot, è possibile non solo rilevare gli attacchi in corso ma anche acquisire preziose informazioni sul comportamento degli aggressori. Ciò

include dati come gli indirizzi IP utilizzati dagli attaccanti e le modalità con cui cercano di ottenere l'accesso non autorizzato. Questa raccolta di informazioni fornisce un'opportunità unica per comprendere le tattiche, le tecniche e le procedure (TTP) utilizzate dagli aggressori, alimentando così una strategia di difesa informata e mirata.

L'utilità del componente di deception non si limita alla sola dissuasione degli attacchi, ma si estende anche alla possibilità di anticipare e comprendere le minacce emergenti. La capacità di simulare ambienti e risorse fittizie offre una prospettiva privilegiata sulla natura mutevole delle minacce cibernetiche, consentendo agli amministratori di sistema di adottare misure preventive mirate e di rafforzare la sicurezza complessiva del sistema.

Sviluppi futuri

Stiamo lavorando su diverse migliorie per il progetto. In futuro, prevediamo di implementare la generazione avanzata di file con LLAMA, integrare la build e l’avvio delle immagini Docker anche se è stata scelta l'autenticazione LDAP, e introdurre un componente interattivo per il monitoraggio dei log. Queste aggiunte mirano a rendere il sistema più efficiente, sicuro e facilmente monitorabile, offrendo un'esperienza più completa agli utenti.

Bibliografia

[1] «Samba.org,» [Online]. Available: https://www.samba.org. [Consultato il giorno 5 Dicembre 2023].

[2] «Wikipedia,» [Online]. Available: https://it.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol. [Consultato il giorno 5 Dicembre 2023].

[3] «Python.org,» [Online]. Available: https://www.python.org. [Consultato il giorno 5 Dicembre 2023].

[4] «Docker.com,» [Online]. Available: https://www.docker.com. [Consultato il giorno 5 Dicembre 2023].

[5] «Ubuntu.com,» [Online]. Available: https://ubuntu.com. [Consultato il giorno 5 Dicembre 2023].

[6] «Pandoc.org,» [Online]. Available: https://pandoc.org. [Consultato il giorno 5 Dicembre 2023].

[7] «Wikipedia,» [Online]. Available: https://it.wikipedia.org/wiki/Kerberos. [Consultato il giorno 5 Dicembre 2023].

[8] «"NTLM." n.d. HackTricks,» [Online]. Available: https://book.hacktricks.xyz/windows-hardening/ntlm.. [Consultato il giorno 13 Dicembre 2023].

[9] «"CVE-2018-1057.",» [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1057.. [Consultato il giorno 13 Dicembre 2023].

[10] «CVE-2023-0922,» [Online]. Available: https://www.samba.org/samba/security/CVE-2023-0922.html. [Consultato il giorno 12 Dicembre 2023].

[11] «keepersecurity,» [Online]. Available: https://www.keepersecurity.com/it_IT/resources/glossary/what-is-kerberos/. [Consultato il giorno 15 Dicembre 2023].