Esercizio bonus W17D4 – Ricerca su GTFOBins, PwnKit e Knockd.

GTFOBins.

GTFOBins, che significa "get the fuck out binaries" è una serie di binari Unix che possono essere sfruttati dagli attaccanti per superare restrizioni alla sicurezza ed eseguire una privilege escalation, una command execution o avere accesso a dei file. Per binario si intendono dei file eseguibili che contengono del codice binario che non ha bisogno di un interprete o compilatore per essere eseguito dal processore. Questi binari sono utilities di sistema presenti di default nei sistemi Unix, come ad esempio Linux e per questo non è difficile utilizzare questi binari in modo malevolo per un exploit, ad esempio per una privilege escalation, per la manipolazione dei file, per eseguire del codice arbitrario, per estrarre dei file, per stabilire delle connessioni con scopi malevoli e per muoversi lateralmente in una rete. Tutte queste azioni sono nascoste dall'uso di binari del tutto insospettabili installati di default nei sistemi. La loro conoscenza è utilissima per chi si occupa di cybersecurity, perché permette di adottare degli accorgimenti per far sì che l'uso di questi binari sia più sicuro e non venga sfruttato dagli attaccanti. Citare qualche esempio di GTFOBins è utile per capire come sia facile sfruttarli e come le conseguenze di un loro utilizzo da parte di un malintenzionato possa essere molto pericolose. Con "find . /bin/sh \; -quit" si riesce ad aprire una shell. I binari SUID sono utili per eseguire dei comandi come il proprietario del binario, che ha solitamente privilegi di root, indipendentemente dall'utente che esegue il comando. Abusando di questa tipologia, è possibile creare una shell, sfruttando /bin/bash/ oppure manipolare dei file importanti come /etc/passwd ed /etc/shadow, modificando gli utenti e le password per scopi malevoli. Esistono anche altri modi per ottenere una shell, ad esempio con l'editor di testo vim si può modificare un file aggiungendo :!bash ed aprire una shell con i privilegi dell'utente corrente. Find potrebbe servire per far eseguire del codice arbitrario con l'option -exec ed anche tar si presta per far ottenere una shell ad un attaccante. GTFOBins è proprio un catalogo di questi binari particolari e fa capire come anche dei binari innocui possano essere utilizzati per compromettere un sistema. Andando più nel dettaglio, per una privilege escalation, si può sfruttare sudo che, se non è configurato esattamente, può portare a delle conseguenze negative. Combinando sudo con less, specialmente se less si esegue con privilegi di root, si può aprire una shell con !sh. Con tar è possibile riuscire ad avere accesso, leggere e modificare dei file senza avere i regolari permessi per farlo. GTFOBins è utile anche per un ambiente nel quale si utilizza Docker per separare i contenuti tra i vari utenti e creare degli ambienti isolati dall'host, e il comando less aiuta a vedere dei file al di fuori del proprio container, magari file sensibili collegati direttamente all'host. Molto spesso, questi binari sono utilizzati come parte di attacchi strutturati, ad esempio si sfrutta una vulnerabilità del kernel come Dirty Pipe (CVE-2022-0847) per avere accesso alla macchina, si fa una privilege escalation utilizzando GTFOBins, poi ci si accerta di poter rimanere sul sistema con crontab e infine si sfrutta il movimento laterale per spostarsi da un host all'altro. Tra le strategie per difendersi e prevenire lo sfruttamento malevolo di questi binari c'è il controllo periodico dei binari SUID, rafforzare i controlli delle azioni eseguite con

i binari tramite Madatory Access Control (MAC) Frameworks come AppArmor e SELinux, usare tool come Aide o Tripwire per accertarsi che file critici di sistema non siano stati alterati, mantenere sotto controllo i log ed aggiornare periodicamente i sistemi.

PwnKit

PwnKit è una vulnerabilità critica per una privilege escalation locale, indicata dal codice CVE-2021-4034, trovata nell'utility Polkit (pkexec) che si trova nella maggior parte dei sistemi Linux. Ha destato preoccupazione fin dalla sua scoperta nel 2022 da parte dei ricercatori del laboratorio Qualys proprio perché è molto diffusa, facilmente sfruttabile e può portare importanti danni. Polkit o PolicyKit è un servizio di sistema presente nei sistemi Unix e similari che permette ai processi senza particolari privilegi di comunicare con processi con privilegi elevati in modo sicuro ed è un toolkit che in generale aiuta a definire le autorizzazioni per i processi in sistemi Unix e similari. Invece di dare subito dei privilegi elevati come nel caso di sudo, Polkit consente un approccio più graduale e granulare, dato che esamina singolarmente le azioni che richiedono privilegi più elevati. Pkexec è una utility che fa parte di Polkit che permette ad un utente autorizzato di eseguire comandi come un altro utente, spesso con privilegi di root. Mentre con sudo è sempre necessario che ogni utente per ogni comando inserisca la giusta password, con pkexec non viene richiesto sempre un permesso esplicito per ogni azione di ogni utente e quindi la privilege escalation diventa più semplice. CVE-2021-4034 è una vulnerabilità causata da una gestione della memoria impropria con pkexec, e questo è dovuto al fatto che l'input non viene validato (specie se non si inseriscono altri argomenti da linea di comando) e quindi vengono manipolate le variabili ambientali, consentendo di manipolare il path ed eseguire dei binari malevoli. Questa problematica relativa alle variabili ambientali porta ad una corruzione della memoria, permettendo di eseguire del codice arbitrario malevolo; un attaccante che riesce a manipolare le variabili ambientali è in grado di far eseguire codice arbitrario con privilegi di root. È una vulnerabilità molto diffusa perché presente di default in quasi tutte le distribuzioni Linux e quindi diffusa nei sistemi Ubuntu, Debian, Fedora e CentOS e diventa pericolosa nei sistemi multi utente, perché permette di avere accesso alle risorse e ai privilegi di altri utenti ed anche di prendere il controllo di tutto l'host, se non sono configurate correttamente le protezioni tra l'host e i vari utenti con i loro privilegi. In linea di massima, il primo passo per sfruttare questa vulnerabilità consiste nell'avere accesso al sistema tramite un account utente manomesso, poi vengono manipolate le variabili ambientali come PATH per eseguire dei comandi arbitrari e poi si lancia pkexec senza argomenti o con un input calcolato per sfruttare le vulnerabilità della memoria e completare così la privilege escalation. Questa vulnerabilità è molto pericolosa, ma è possibile porvi rimedio in vari modi. Per prima cosa, sono già state rilasciate delle patch di aggiornamento che vanno a sanitizzare le variabili ambientali e che correggono le vulnerabilità della gestione della memoria. Si possono scaricare con un sudo apt update && sudo apt upgrade. Se pkexec non è necessario e serve una misura di mitigazione rapida, è possibile disabilitare pkexec, rimuovendolo del tutto o rendendolo non eseguibile con chmod 0750 /usr/bin/pkexec. È utile anche usare tool di audit per monitorare eventuali attività sospette che possono essere alla base di un privilege escalation e limitare l'accesso

locale, per evitare che utenti non autorizzati e non sicuri possano accedere al sistema con intenzioni malevole. Gli indicatori che devono far sospettare di un exploit di questa vulnerabilità sono la modifica o la creazione di file con path come /tmp o /var/tmp o nella directory home di un qualche utente, la creazione di nuovi account users o la modifica di quelli esistenti (da analizzare nei file /etc/passwd ed /etc/shadow), modifiche o cancellazioni sospette nei log e modifiche nei crontab jobs, che possono richiede alla macchina di eseguire del codice malevolo in un momento preciso o ad intervalli stabiliti.

Knockd

Knockd è un demone, un tool software che implementa il port knocking, una tecnica utilizzata per controllare gli accessi ad un server che prevede che il firewall del server tenga chiuse e nascoste le porte fino a che non riceve una serie specifica di tentativi di connessione a delle determinate porte, detta anche "knock sequence". Quando la corretta sequenza di knock viene lanciata da parte di un utente che la conosce, le porte, come quella di SSH, vengono aperte e permettono all'utente autorizzato di compiere le azioni di cui ha bisogno. Knockd monitora i log del firewall per trovare delle sequenze di knocking su porte chiuse e capisce, in base alla sua configurazione, che azione deve eseguire in base alla sequenza rilevata. Si integra quindi con il firewall in modo da aumentare il livello di sicurezza delle porte, aprendole solo quando serve con utenti verificati anziché lasciarle sempre aperte a maggiori rischi. Knockd prevede una sequenza di knock, ovvero una sequenza di connessioni a determinate porte ben definita e riconoscibile e un demone in ascolto sul server per trovare le sequenze di knock stabilite ed eseguire le azioni con cui è configurato. Le configurazioni si trovano nel file /etc/knockd.conf e aiutano knockd ad eseguire diverse azioni, come aprire temporaneamente una porta, chiuderla oppure inviare un alert in caso di tentativi di accesso sospetti e questo aiuta a proteggere delle porte non visibili pubblicamente. Le sequenze di knock possono riguardare una porta singola o porte multiple e quest'ultima soluzione è da preferire, perché un attaccante potrebbe riuscire a scoprire la porta singola a cui connettersi, mentre è molto più complesso portare avanti un brute force o intercettare una sequenza di porte a cui collegarsi. È bene scegliere una sequenza lunga, per esempio di 5 porte, per poter ostacolare un possibile brute force, combinare protocolli TCP ed UDP nella frequenza ed inserire dei ritardi per rendere più complicata l'identificazione della sequenza giusta da parte di un attaccante. Knockd contribuisce in modo importante alla sicurezza, perché evita che sia possibile una scansione completa delle porte e dei servizi da parte degli attaccanti, celando le porte agli utenti esterni, aprendole solo con la giusta sequenza di knock e richiudendo le porte dopo che l'azione necessaria è stata portata a termine. Knockd offre un servizio aggiuntivo di protezione senza richiedere particolari risorse hardware o una complicata configurazione e riduce significativamente la superficie di attacco perché consente di nascondere delle porte specifiche o sensibili. Bisogna però evitare di inserire delle sequenze troppo scontate di knock, includendo molte porte, protocolli diversi e dei ritardi ed aggiungere una cifratura o una qualche tecnica di offuscamento per evitare che un attaccante sniffi il traffico network e riesca a ricostruire la sequenza di knock riuscendo ad avere accesso a porte sensibili. Knockd viene utilizzato molto spesso in casi specifici, ad

esempio per nascondere e limitare l'accesso alla porta 22 di SSH o per controllare meglio l'accesso a servizi web come http ed FTP, alla base di vulnerabilità comunemente sfruttate per gli attacchi.