

GTFOBins, PwnKit, e knockd

Cari guerrieri della sicurezza cibernetica, Il Concilio degli Arcimaghi del Cyberspazio ha emesso una chiamata urgente. Una Torre arcana, protetta da incantesimi oscuri, nasconde al suo interno tre reliquie di immensa potenza: GTFOBins, PwnKit, e knockd. Questi artefatti contengono segreti antichi che, se compresi e utilizzati correttamente, vi permetteranno di difendere le vostre reti da minacce insidiose.

Gli Artefatti

1. GTFOBins: Questo è un grimorio di incantesimi che permette ai potenti maghi del Cyberspazio di sfruttare strumenti di sistema apparentemente innocui per ottenere il controllo completo su macchine vulnerabili. Solo chi conosce gli incantesimi e le combinazioni giuste può evocarne il potere.
2. PwnKit: Si narra che questa reliquia contenga un exploit leggendario, noto come Polkit, che consente a chi lo padroneggia di innalzarsi da umili diritti di utente a poteri amministrativi completi. Chiunque riuscirà a decifrare il suo funzionamento potrà controllare qualsiasi sistema con accesso limitato.
3. knockd: Protetto da un incantesimo di invisibilità, questo artefatto consente ai maghi di camuffare le loro azioni, facendo apparire le loro incursioni come invisibili agli occhi dei guardiani della rete. Solo coloro che comprendono il suo linguaggio segreto potranno utilizzarlo per aprire le porte ai reami nascosti senza essere visti.

-
1. Il primo artefatto GTFOBins : L'artefatto GTFOBins si manifesta come un antico grimorio, un libro di incantesimi consumato dal tempo, con una copertina ricoperta di rune e simboli che brillano di una luce

spettrale. Le pagine sono aperte, rivelando un intricato intreccio di codici terminali e comandi criptici, che sembrano essere scritti in un linguaggio tanto arcano quanto pericoloso. Il libro emana un'aura oscura, circondato da ombre che sembrano danzare al ritmo di una melodia invisibile. Nella parte superiore dell'immagine, il nome GTFOBins è inciso in una fonte arcana e luminosa, ben visibile contro lo sfondo tenebroso, che evoca una sensazione di mistero e potere latente. Lo sfondo stesso è una fusione di elementi cyber e arcani, con circuiti digitali appena visibili, intrecciati con trame magiche, suggerendo la natura duale e ingannevole dell'artefatto. Questo artefatto è simbolo di potere nascosto, accessibile solo a coloro che possiedono la conoscenza necessaria per svelarne i segreti, utilizzandolo come strumento di controllo o difesa nelle guerre cibernetiche.



2. Il secondo artefatto PWNKIT: L'artefatto PwnKit si presenta come una chiave antica, sospesa nell'aria, circondata da un'aura luminosa che sembra pulsare di potere arcano. La chiave è riccamente incisa con intricati simboli e rune, che brillano di una luce dorata, suggerendo la sua natura preziosa e potente. La forma della chiave è elegante e complessa, evocando antichi segreti e meccanismi nascosti che solo chi possiede la chiave può sbloccare. Il nome PwnKit è scolpito in una

font arcana, anch'essa luminosa, posizionata nella parte superiore dell'immagine, ben visibile contro lo sfondo oscuro e misterioso. L'ambiente circostante è avvolto in ombre dense, con vaghi suggerimenti di meccanismi antichi e strutture cibernetiche che si fondono con l'oscurità, creando un'atmosfera di mistero e potenziale minaccia. Questo artefatto è simbolo di accesso e dominio, capace di elevare chi lo possiede a un livello di controllo totale sui sistemi a cui viene applicato. È un oggetto di grande potenza, ma che richiede saggezza e cautela nell'uso, poiché un potere così grande può facilmente sfuggire al controllo di chi lo impugna.



-
3. Il terzo artefatto KNOCKD L'artefatto knockd appare come un enigmatico lockbox antico, avvolto in mistero e segretezza. Il lockbox è realizzato in un metallo scuro, forse ossidato dal tempo, con rune e simboli arcani incisi sulla sua superficie, che emanano un tenue bagliore bluastro. La scatola è leggermente aperta, con una luce fievole che filtra dall'interno, suggerendo che al suo interno siano celati segreti o poteri sconosciuti. Il nome knockd è inciso nella parte

superiore dell'immagine, in una fonte luminosa e arcana, ben definito contro il fondo oscuro e nebuloso. Lo sfondo dell'immagine è avvolto in un'oscurità profonda, con ombre che si muovono appena visibili, creando un'atmosfera di suspense e tensione. Sottili elementi cibernetici, come circuiti e schemi digitali, si intrecciano con le ombre, evocando la natura segreta e furtiva dell'artefatto. Questo artefatto rappresenta la chiave per accedere a reami nascosti e protetti, permettendo a chi lo comprende di operare inosservato e di rivelare passaggi segreti solo a coloro che conoscono il giusto codice. È uno strumento di grande valore per chi cerca di proteggere o accedere a informazioni riservate, operando nell'ombra senza destare sospetti.



Ecco il testo formattato correttamente con l'inclusione del codice:

GTFOBins – Descrizione e Uso

GTFOBins (Get The F**k Out Binaries) è un progetto open-source che raccoglie un elenco di binari preinstallati nei sistemi UNIX, i quali possono

essere sfruttati per bypassare le restrizioni di sicurezza e ottenere l'escalation dei privilegi. Questi binari, considerati innocui, possono essere utilizzati per eseguire comandi malevoli, ottenere una shell o accedere a file riservati.

Uso e Funzionalità:

GTFOBins si concentra sui binari che possono essere usati per:

- **Escalation dei privilegi:** Alcuni binari possono essere usati per ottenere i permessi di root o altri privilegi elevati.
- **Bypass dei permessi:** Utilizzo di binari per leggere o modificare file protetti.
- **Esecuzione di comandi remoti:** Possono essere eseguiti comandi arbitrari o aperte backdoor.
- **Persistenza:** Creare meccanismi per mantenere l'accesso persistente a un sistema compromesso.

Esempio:

Un esempio famoso è l'uso del binario `tar`, che può essere utilizzato per ottenere una shell interattiva con privilegi elevati in determinati contesti:

```
tar -cf archive.tar --checkpoint=1 --checkpoint-
action=exec=/bin/sh
```

Come usarlo:

Attaccanti e penetration tester utilizzano GTFOBins per trovare metodi di exploit su sistemi con binari male configurati. Puoi visitare il sito ufficiale [GTFOBins](#) per cercare binari specifici e le relative vulnerabilità.

PwnKit – Descrizione e Uso

PwnKit (CVE-2021-4034) è una vulnerabilità critica identificata nel pacchetto Polkit, un componente chiave nei sistemi Linux che gestisce i privilegi di accesso a livello di sistema. La vulnerabilità è stata scoperta nei primi mesi del 2022 e permette agli attaccanti locali di ottenere i privilegi di root senza autenticazione.

Dettagli Tecnici:

Il problema riguarda il binario `pkexec`, che permette l'esecuzione di comandi come superutente. La vulnerabilità permette agli attaccanti di manipolare l'input e causare l'esecuzione di comandi arbitrari con privilegi di root.

Esempio di Exploit:

L'exploit tipico di PwnKit consiste nell'eseguire `pkexec` senza argomenti o con argomenti malformati.

```
pkexec --version
```

Se la versione è vulnerabile, puoi sfruttare la vulnerabilità compilando ed eseguendo un exploit:

```
gcc pwnkit_exploit.c -o pwnkit_exploit  
./pwnkit_exploit
```

Soluzione:

- **Aggiornare Polkit** alle versioni patchate che risolvono la vulnerabilità.

- **Rimuovere temporaneamente** `pkexec` fino all'aggiornamento del sistema.
-

knockd – Descrizione e Uso

knockd è un demone che implementa la tecnica del **port knocking**, utilizzata per migliorare la sicurezza delle connessioni a servizi remoti. Il port knocking è un meccanismo in cui un server firewall blocca completamente le porte, ma le apre temporaneamente se riceve una sequenza specifica di richieste sulle porte chiuse.

Come funziona:

Un utente remoto "bussa" su una serie predefinita di porte inviando pacchetti TCP, UDP o ICMP. Il demone knockd riconosce questa sequenza e apre una porta, ad esempio la porta 22 (SSH), permettendo l'accesso.

Configurazione:

Un file di configurazione di knockd potrebbe sembrare così:

```
[openSSH]
sequence = 7000,8000,9000
tcpflags = syn
command = /sbin/iptables -A INPUT -s %IP% -p tcp --dport 22 -j
ACCEPT
```

Quando knockd riceve una sequenza di pacchetti TCP SYN sulle porte 7000, 8000 e 9000, apre la porta 22 per l'indirizzo IP che ha inviato la sequenza.

Pro e Contro:

- **Pro:**
 - Nasconde i servizi critici dietro porte chiuse.
 - Previene scansioni automatiche delle porte.
 - **Contro:**
 - Vulnerabile a replay attack se la sequenza non cambia.
 - Se qualcuno intercetta la sequenza, può sfruttarla per accedere al sistema.
-

Configurazione di knockd in Kali Linux

1. Passo 1: Installa knockd (se non è già installato)

Installare il pacchetto knockd su Kali Linux:

```
sudo apt install knockd
```

2. Passo 2: Configura il file /etc/knockd.conf

Configura il file `/etc/knockd.conf` per gestire le sequenze di knocking e aprire la porta SSH:

```
[openSSH]
sequence = 7000,8000,9000
seq_timeout = 5
command = /sbin/iptables -A INPUT -s %IP% -p tcp --dport 22 -j
ACCEPT
tcpflags = syn
```

3. Passo 3: Avvia knockd

Avvia il servizio knockd per attivare la configurazione:

```
sudo service knockd start
```

Passo 4: Usa knock per inviare la sequenza di "bussate"

Dopo aver configurato knockd, invia la sequenza corretta di knock per aprire la porta SSH:

```
knock <IP_destinazione> 7000 8000 9000
```

Riassunto

1. **GTFOBins**: Una raccolta di binari utilizzabili per eseguire exploit come l'escalation di privilegi o l'accesso a risorse protette sui sistemi UNIX.
2. **PwnKit**: Una vulnerabilità critica nel binario `pkexec` di Polkit che permette l'escalation di privilegi su sistemi Linux.
3. **knockd**: Un demone per implementare il port knocking, una tecnica di sicurezza che apre porte specifiche in base a una sequenza di richieste.

Conclusioni

GTFOBins, PwnKit e knockd evidenziano l'importanza di una corretta configurazione e gestione della sicurezza nei sistemi operativi. GTFOBins dimostra come binari comuni possano essere sfruttati in modo malevolo, mentre PwnKit sottolinea la criticità delle vulnerabilità nei componenti di sistema. Infine, knockd mostra come tecniche creative possano aumentare la sicurezza nascondendo porte sensibili.

Per una strategia di sicurezza efficace, è essenziale un approccio difensivo su più livelli, combinando aggiornamenti regolari con il monitoraggio e la consapevolezza delle ultime minacce.

L'uso di strumenti come **GTFOBins**, **PwnKit** e **knockd** come componenti per un firewall potrebbe sembrare insolito, dato che non sono progettati direttamente per la protezione di un sistema, ma per scopi offensivi o di gestione delle vulnerabilità. Tuttavia, è possibile immaginare scenari in cui alcuni dei concetti e delle tecniche utilizzate da questi strumenti possano essere applicati per rafforzare la sicurezza di un firewall o per proteggere un sistema. Vediamo come potrebbero essere utilizzati in questo contesto:

1. GTFOBins come guida per la configurazione del firewall

GTFOBins evidenzia binari legittimi preinstallati nei sistemi UNIX/Linux che possono essere sfruttati per bypassare le restrizioni di sicurezza, soprattutto quando sono mal configurati. Questi binari potrebbero essere utilizzati come riferimento per rafforzare le policy di sicurezza del firewall.

Utilizzo nel contesto del firewall:

- **Monitoraggio e controllo:** Un firewall potrebbe essere configurato per monitorare e bloccare l'esecuzione di binari sospetti o non necessari che sono comunemente presenti in GTFOBins, prevenendo così possibili tentativi di escalation dei privilegi.
- **Whitelist e blacklist:** Creazione di liste bianche e nere per eseguibili. I binari elencati in GTFOBins, noti per essere sfruttabili, potrebbero essere aggiunti a una lista di controllo per monitorarne l'accesso o limitarne l'uso tramite il firewall.
- **Restrizioni sugli utenti:** Potrebbe essere limitato l'accesso a binari con setuid attivo o configurare regole firewall che blocchino l'uso di binari potenzialmente pericolosi per utenti non privilegiati.

2. PwnKit come avvertimento per la sicurezza del firewall

PwnKit rappresenta una vulnerabilità critica legata alla gestione dei privilegi su Linux tramite il comando `pkexec`. Un firewall ben configurato potrebbe rilevare e mitigare eventuali tentativi di sfruttare vulnerabilità simili attraverso il monitoraggio delle attività di sistema.

Utilizzo nel contesto del firewall:

- **Monitoraggio dei comandi privilegiati:** Un firewall configurato con regole di monitoraggio potrebbe intercettare richieste di esecuzione di comandi con `pkexec` o altri eseguibili privilegiati, soprattutto quando sono eseguiti da utenti non privilegiati o senza un motivo evidente.
- **Gestione delle vulnerabilità:** I firewall avanzati possono essere configurati per riconoscere e bloccare exploit noti come quelli di PwnKit, impedendo così l'escalation dei privilegi all'interno del sistema.
- **Protezione basata su firme:** Un firewall potrebbe utilizzare firme di exploit noti per rilevare quando viene tentato un attacco PwnKit, bloccando il traffico o l'esecuzione di comandi associati.

3. knockd per migliorare la sicurezza del firewall

knockd è un demone che implementa il **port knocking**, una tecnica in cui le porte di un server vengono aperte solo dopo che è stata ricevuta una sequenza predefinita di tentativi di connessione. Questa tecnica potrebbe essere direttamente applicata in un contesto di firewall per nascondere i servizi critici.

Utilizzo come parte di un firewall:

- **Port Knocking:** Un firewall potrebbe essere configurato per implementare la tecnica del port knocking, aprendo le porte solo a seguito di una sequenza specifica di tentativi di connessione, il che aggiunge un ulteriore strato di protezione contro gli attacchi di scansione delle porte.
- **Accesso condizionato:** Il firewall potrebbe consentire l'accesso a servizi come SSH, VPN, o RDP solo dopo che è stata ricevuta la sequenza corretta di knock, nascondendo i servizi critici fino a quando un utente autorizzato esegue la sequenza.
- **Difesa contro gli attacchi automatizzati:** Il port knocking aiuta a prevenire gli attacchi di brute force o le scansioni automatizzate, poiché le porte appaiono chiuse fino a quando non viene "bussato" correttamente.

Utilizzo combinato per migliorare la sicurezza del firewall:

1. **Limitazione dell'accesso ai binari di sistema:** Usando l'analisi dei binari sfruttabili presenti in GTFOBins, potresti impostare il firewall per monitorare o limitare l'accesso a binari specifici (come `tar`, `vim`, `nano`, `find`, ecc.), riducendo le superfici di attacco.
2. **Rilevamento di exploit noti:** Il firewall potrebbe monitorare il traffico di rete e le attività del sistema alla ricerca di exploit noti, come quelli di PwnKit, e bloccare tentativi sospetti di esecuzione di comandi privilegiati.
3. **Port Knocking avanzato con logging e monitoraggio:** Implementare il port knocking con `knockd` come parte integrante del firewall, potresti rafforzare la sicurezza, monitorando e loggando tutti i tentativi di knock e invalidando le sequenze dopo un determinato numero di tentativi falliti.

Vantaggi dell'integrazione:

- **Riduzione delle superfici di attacco:** Il firewall può bloccare binari e vulnerabilità noti sfruttati comunemente in attacchi, riducendo così il rischio complessivo di compromissione.
- **Nascondere servizi critici:** Grazie al port knocking, il firewall può nascondere le porte critiche fino a quando non vengono eseguite operazioni di knocking valide.
- **Monitoraggio delle attività sospette:** La combinazione di monitoraggio delle attività di sistema e il controllo dei binari potrebbe rilevare attività sospette che indicano tentativi di sfruttamento di vulnerabilità.

Svantaggi e sfide:

- **Port Knocking vulnerabile:** Se non configurato correttamente, il port knocking potrebbe essere soggetto a replay attack o attacchi di forza bruta.
- **Complessità di configurazione:** Integrare queste tecniche richiede una configurazione accurata e un monitoraggio costante, che potrebbe aumentare la complessità operativa.
- **Risorse di sistema:** Monitorare costantemente l'uso di binari o rilevare exploit può richiedere un notevole consumo di risorse, soprattutto su sistemi ad alta intensità di traffico.

Conclusione

L'integrazione dei concetti e delle tecniche utilizzate in **GTFOBins**, **PwnKit** e **knockd** in un firewall avanzato potrebbe rafforzare la sicurezza di un sistema operativo. Tuttavia, queste tecniche devono essere applicate con

attenzione, configurate correttamente e accompagnate da un monitoraggio costante per garantire una protezione efficace.