

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.



GTFOBins – Descrizione e Uso

GTFOBins è un progetto che raccoglie eseguibili Unix che possono essere sfruttati per ottenere accesso non autorizzato o privilegi elevati. Molti di questi eseguibili, se configurati in modo errato, consentono azioni come escalation dei privilegi, esecuzione di comandi arbitrari o accesso a file riservati.

Vulnerabilità sfruttate:

GTFOBins sfrutta binari con il bit **setuid** attivato, che permette agli utenti non privilegiati di eseguire operazioni con privilegi elevati, bypassando così le restrizioni di sicurezza.

Mitigazione:

Per mitigare queste vulnerabilità, è importante ridurre al minimo l'uso di binari con setuid attivo e monitorarne l'utilizzo per prevenire abusi.

Uso in Kali Linux:

1. Passo 1: Identifica i binari disponibili sul sistema

Puoi usare il seguente comando per trovare i binari con setuid attivato:

```
find / -perm -4000 2>/dev/null
```

2. Passo 2: Usa uno dei binari GTFOBins per eseguire comandi con privilegi elevati

Se trovi `find` tra i binari:

```
sudo find . -exec /bin/sh ;
```

PwnKit – Descrizione e Uso

PwnKit è una vulnerabilità critica scoperta nel componente **polkit** (PolicyKit), responsabile della gestione dei privilegi nei sistemi Linux. La vulnerabilità CVE-2021-4034 consente a un utente locale non privilegiato di ottenere accesso root sfruttando il comando `pkexec` in modo non autorizzato.

Vulnerabilità sfruttate:

PwnKit sfrutta un bug nella gestione delle variabili d'ambiente di `pkexec`,

consentendo a un attaccante di eseguire codice arbitrario con privilegi root senza necessità di autenticazione.

Mitigazione:

La vulnerabilità può essere mitigata aggiornando `polkit` alla versione che contiene la patch corretta o disabilitando completamente `pkexec` se non è necessario.

Uso in Kali Linux:

1. Passo 1: Controlla la versione di pkexec

Verifica se il sistema è vulnerabile controllando la versione di `pkexec`:

```
pkexec --version
```

2. Passo 2: Scarica o crea l'exploit da eseguire

Se la versione è vulnerabile, puoi sfruttare la vulnerabilità usando uno script exploit. Ecco un esempio di compilazione ed esecuzione di un exploit:

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

3. Mitigazione:

Aggiorna `pkexec` su tutte le macchine vulnerabili con:

```
sudo apt update && sudo apt upgrade
```

knockd – Descrizione e Uso

knockd è uno strumento utilizzato per implementare la tecnica di **port knocking**, che permette di nascondere i servizi di rete dietro un firewall e di

aprire una porta solo dopo che una sequenza predefinita di tentativi di connessione (knock) è stata inviata. Ad esempio, la porta SSH può rimanere chiusa finché non viene "bussato" alle porte corrette.

Vulnerabilità sfruttate:

Se un attaccante riesce a scoprire la sequenza di knock, può accedere ai servizi nascosti senza ulteriori autenticazioni, violando la sicurezza del sistema.

Mitigazione:

La mitigazione consiste nel creare sequenze di knock lunghe e complesse per ridurre le probabilità di forza bruta. Inoltre, è importante monitorare costantemente i tentativi di connessione e gli accessi.

Configurazione e Utilizzo in Kali Linux:

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

Per installare knockd su Kali Linux:

```
sudo apt install knockd
```

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

Ecco un esempio di configurazione per aprire la porta SSH solo dopo aver "bussato" alle porte 7000, 8000, e 9000:

```
[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 demone knockd:

```
sudo service knockd start
```

4. 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
```