Relazione sulla Gestione della Backdoor sulla Porta 1524 di Metasploitable

Introduzione

Sulla macchina Metasploitable, è stato rilevato un servizio in esecuzione sulla porta 1524 che offre una shell remota non autorizzata. Questo rappresenta una backdoor pericolosa che può essere sfruttata da attaccanti per ottenere accesso non autorizzato al sistema. Questa relazione spiega come identificare e terminare il processo responsabile dell'apertura della backdoor e come mettere in sicurezza il sistema.

Identificazione del Processo che Apre la Backdoor

Per identificare il processo che sta aprendo la backdoor sulla porta 1524, ho eseguito i seguenti passaggi:

1. **Verificare le connessioni attive sulla porta 1524**:
2. **Visualizzare i dettagli del processo**:

Terminare il Processo

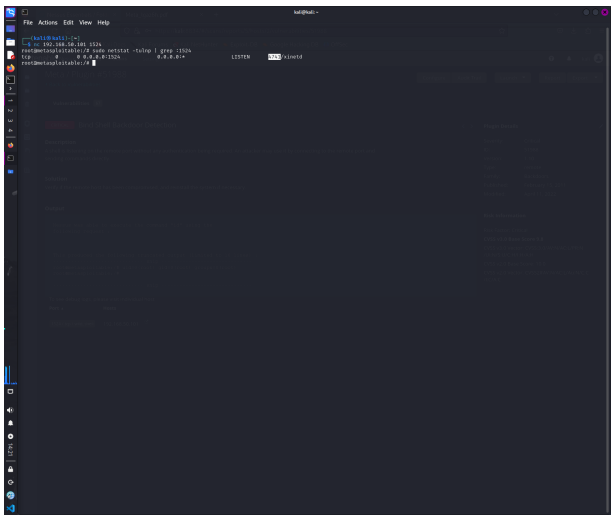
Per interrompere il processo responsabile della backdoor, ho eseguito il comando `kill`:

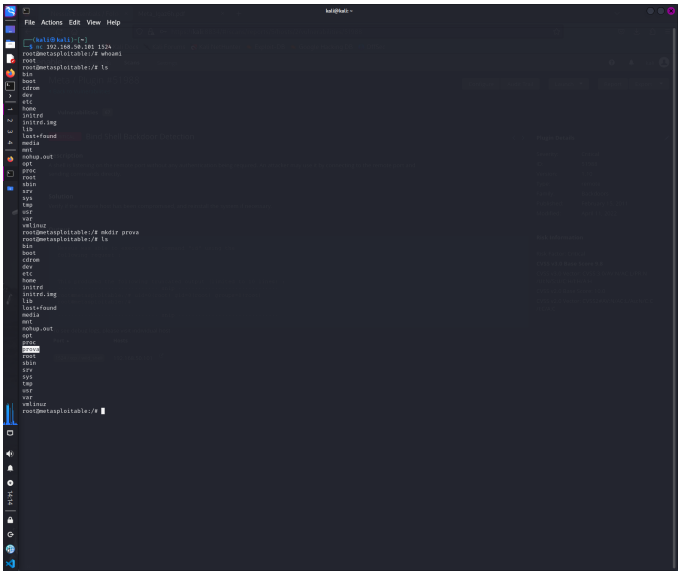
1. **Terminare il processo con il PID identificato (4741)**:
2. **Verificare che il processo non sia più in esecuzione**:

Mettere in Sicurezza il Sistema

Per prevenire il riavvio del servizio e migliorare la sicurezza del sistema:

1. **Rimuovere o commentare la voce corrispondente nel file di configurazione di `inetd`**
   Cercare la riga che definisce il servizio sulla porta 1524 commentarla aggiungendo un `#` all'inizio della riga o eliminandola.
2. **Riavviare il servizio `inetd`** per applicare le modifiche:
3. **Aggiungere regole firewall per bloccare l'accesso alla porta 1524**:





Relazione sulla Messa in Sicurezza del Servizio VNC su Metasploitable

Virtual Network Computing (VNC) è un sistema grafico per il controllo remoto che permette di gestire un computer a distanza. Su Metasploitable, un servizio VNC è in esecuzione e Nessus ha identificato una vulnerabilità critica: l'accesso è possibile con una password debole. Questa relazione illustra come mettere in sicurezza il servizio VNC cambiando la password e aggiungendo una regola firewall per gestire il traffico sulla porta VNC (5900).

Cambiare la Password del Servizio VNC

Per migliorare la sicurezza del servizio VNC, il primo passo è cambiare la password utilizzando il comando per diventare root e poi `vncpasswd`.

Verrà richiesto di inserire e confermare una nuova password. Assicurarsi di scegliere una password complessa e difficile da indovinare, includendo una combinazione di lettere maiuscole e minuscole, numeri e simboli.

Aggiungere una Regola Firewall per la Porta 5900

Per aggiungere un ulteriore livello di sicurezza, configurare il firewall per limitare l'accesso alla porta 5900 solo agli indirizzi IP autorizzati.

Implementando queste misure, si può significativamente migliorare la sicurezza del servizio VNC su Metasploitable.

Relazione sulla Configurazione e Messa in Sicurezza di NFS

Introduzione

Network File System (NFS) è un protocollo che consente a un sistema di condividere directory e file con altri sistemi su una rete. Tuttavia, la configurazione predefinita di NFS potrebbe non essere sicura e può esporre i dati a rischi di accesso non autorizzato. Questa relazione illustra come configurare e mettere in sicurezza NFS su un sistema Linux/Unix, concentrandosi sulla configurazione dei file principali e sulla creazione di regole firewall per gestire le connessioni.

Configurazione di NFS

La configurazione di NFS si basa su tre file principali:

1. **/etc/exports**
2. **/etc/hosts.allow**
3. **/etc/hosts.deny**

Il file `/etc/hosts.allow` specifica quali computer sulla rete possono accedere alle share condivise.

Questo permette al sistema con l'IP 192.168.1.100 di accedere ai servizi NFS.

Il file `/etc/hosts.deny` specifica quali computer sulla rete non possono accedere alle share condivise.

Questo blocca l'accesso a tutti i computer, eccetto quelli esplicitamente permessi in `/etc/hosts.allow`.

Creazione di Regole Firewall

Per migliorare la sicurezza, è consigliabile configurare il firewall per limitare le connessioni ai servizi NFS. Utilizzando `iptables` o `firewalld`, possiamo creare regole per permettere l'accesso solo da specifici IP.